INTERNET DOCUMENT INFORMATION FORM

A . Report Title: US Army Year 2000 (Y2K) Action Plan Revision II

B. DATE Report Downloaded From the Internet: 18 Aug 98

C. Report's Point of Contact: (Name, Organization, Address, Office Symbol, & Ph #:) **William H. Campbell**
Lieutenant General, GS
Army CIO
The Pentagon
Washington, DC

D. Currently Applicable Classification Level: Unclassified

E. Distribution Statement A: Approved for Public Release

F. The foregoing information was compiled and provided by:
DTIC-OCA, Initials: __PM__ **Preparation Date**: 18 Aug 98

The foregoing information should exactly correspond to the Title, Report Number, and the Date on the accompanying report document. If there are mismatches, or other questions, contact the above OCA Representative for resolution.

US Army

Year 2000 (Y2K)

Action Plan
Revision II

June 1998

TABLE OF CONTENTS

1. PURPOSE 6

2. BACKGROUND 6

3. MISSION CRITICAL SYSTEMS 7

4. ARMY Y2K MANAGEMENT STRATEGY 8

5. INSTALLATION AND GARRISON COMMANDERS 10

6. PRIORITIZING SYSTEMS AND DEVICES 11

7. Y2K RISK MANAGEMENT 11

8. U. S. ARMY YEAR 2000 DATA BASE (USAY2KDB) 14

9. ONE-LINER SYSTEMS AND DEVICES REPORTING REQUIREMENTS 16

10. USAY2KDB ENTRY EXAMPLES 16

11. COMPLIANCE CERTIFICATION CHECKLIST 17

12. CONTRACTUAL ISSUES 17

13. SCHEDULE - THE Y2K FIVE-PHASE RESOLUTION PROCESS 18

14. INTERFACE AGREEMENTS 18

15. RESPONSIBILITIES 19

APPENDIX A: GLOSSARY 28

APPENDIX B: THE Y2K FIVE-PHASE RESOLUTION PROCESS 30

APPENDIX C: COMPLIANCE DEFINITION - AS OF 1 JAN 1997 31

APPENDIX D: CONTRACT LANGUAGE 32

APPENDIX E: Y2K MISSION CRITICAL SYSTEM - LATE REPORT 34

APPENDIX F: Y2K CERTIFICATION CHECKLIST 35

TABLE OF CONTENTS

APPENDIX G: INFRASTRUCTURE RISK ASSESSMENT GUIDANCE 48
APPENDIX H: SAMPLE MOA (INTERFACE AGREEMENT) 64
APPENDIX I: SAMPLE Y2K RISK MANAGEMENT PLAN 65
APPENDIX J: SAMPLE Y2K RISK MANAGEMENT WORKSHEET 69
APPENDIX K: Y2K SYSTEM OR DEVICE CONTINGENCY PLAN OUTLINE.....71
APPENDIX L: Y2K COST ESTIMATING GUIDANCE 75
APPENDIX M: Y2K COST FACTORS CHECKLIST 76

FORWARD

The Year 2000 (Y2K) problem stems from the use of two-digit year fields instead of four digit year fields in software, hardware, and firmware, including embedded chips. This will cause many computer programs and devices to fail as they attempt to calculate against the year "00" not recognizing that the year is actually 2000. The resulting inaccuracies in date-related calculations will generate corrupt data results and will cause some systems to fail entirely. If erroneous information goes unrecognized, the problem is perpetuated through interfaces with other systems. While this is the basis of the problem, it is actually more complex. Many systems and devices with embedded information technology (IT) have faulty date logic that does not recognize that the Y2K is a leap year. Some systems use the code "00 or 99" as a trigger to execute an action, while others, such as the Global Positioning System (GPS), have overflow or rollover problems.

The Y2K problem is not limited to any one functional area within the Army. We use computers to support or actually perform every function we conduct. From our business functions such as financial, personnel, contract, and logistics management, to the performance and support of our strategic and tactical operations such as mobilizing, deploying, and maneuvering forces, we rely on computers. Information systems and devices are used to support intelligence, surveillance, security, weapons, and weapons systems deployment. The Army has never faced such a problem. In view of the extraordinary magnitude and seriousness of the problem, the Army must react in kind.

The effort to correct Army systems and devices affected by Y2K is daunting. To be successful, senior level managers must be personally involved. We must dedicate adequate resources to correct Y2K issues and manage the effort. The Army will not assign Y2K as an "extra duty." It is important to not only assign enough people to the job, but to also be sure they are the right people with the proper mix of management and technical skills. Y2K poses a tremendous near term challenge to the Army, DoD, the nation, and the world. The Y2K resolution deadline is unforgiving. Senior leaders must continue to take personal interest in the resolution of Y2K problems, because you will be held personally responsible for the success or failure of Y2K efforts in your organization. Put your top people on the job, hold regular status meetings, review progress, review your organization's data submittals, put controls in place that will ensure data is submitted on time, review system and device correction progress against schedules, review system and device risk assessments, ensure contingency plans are in place and are feasible, and prepare for Y2K compliance testing. Get personally involved, and stay involved.

The Y2K Project Office has revised this action plan to provide a roadmap to success. A plan is only as good as the resulting actions. It will take strong, dedicated, senior level backing and intense management efforts to put the Army Y2K plan into action. I rely on you, the Department of the Army (DA) Functional Proponents (FPs), the Program Executive Officer's (PEOs), the Major Commands (MACOMs), the installation commanders, Program, Product, Project Managers (PMs), and system owners to read, understand, implement, and perform according to your designated responsibilities. Review this entire plan, paying particular attention to the responsibility section, and take the necessary steps to be sure your organization is performing accordingly. I depend on you to make the plan succeed.

We will work together to ensure Army systems and devices continue to function as planned through 2000, and to ensure the capability to carry out the Army mission is not put in jeopardy. I am positive the Army is up to the challenge.

WILLIAM H. CAMPBELL
Lieutenant General, GS
Army CIO

1.

Purpose

a. The purposes of the Army Year 2000 (Y2K) Action Plan are to outline the Army Y2K management strategy, provide guidance, define roles, define responsibilities, define reporting requirements, and lay a foundation that will ensure no mission critical failures occur due to Y2K-related problems. As in the past, special emphasis is placed on mission critical systems, however, the Army's goal is to correct all Y2K impacted systems and devices. This revision supports the Army and DoD corporate strategy for Y2K resolution.

b. This revision applies to all systems supported by information technology, their technical environment, and their communications devices. Systems include automated business information systems, automated command and control systems, and weapon systems. This revision also applies to infrastructure and devices as defined in the 12 March 1997 ASD(C3I) memorandum and in paragraph 9 of this plan. Information technology support includes hardware, firmware, COTS, GOTS and developed software, and data. Software includes COTS and GOTS packages, operating systems, third and fourth generation language compilers and interpreters, functional applications, system utilities, translators, and database management systems. Data includes databases and other data storage structures and mechanisms, data and system interfaces, Electronic Data Interchange (EDI) transaction sets and implementation conventions, and other messages or forms of data exchange. As the Army moves through the Y2K resolution phases, updates to this plan will be required.

2. Background

a. In the last three decades, many systems were designed to minimize memory and storage requirements due to expense or lack of system capacity. Processor speeds were slow and system life expectancy was short. Thus, the de facto information technology date standard developed using only two digits to represent the year in most cases. Systems representing dates using a two-digit year, i.e., 96 instead of 1996, are the crux of the Y2K problem. Cross century date calculations, comparisons, and sequencing or sorting will fail: 00 - 60 = -60 but 2000 - 1960 = 40! The year 1999 creates additional problems for systems using the digits "99" or "00"in a date field to indicate end-of-file, no expiration, or a trigger for some other action. To add to the problem, many systems have faulty date logic and fail to identify the Y2K as a leap year. Finally, many hardware and operating systems do not roll over correctly from 1999 to 2000.

b.

There are generally three approaches to fixing Y2K problems for information systems. First, the most permanent fix is to expand dates to a four-digit year and modify associated code to use the full four-digit year. The second approach is more temporary, using logic to determine the century in which a two-digit year belongs. Finally, the third approach is to retire, replace, rewrite, or replatform the system. The best approach to use is system dependent. Additional strategies may be found at http://www.mitre.org/research/y2k/docs/straegies.html.

c. Y2K can also impact devices. Devices that may be impacted range from communication switches, building infrastructure items such as security, fire detectors and suppression systems to public utilities. Often fixing devices will depend on vendor plans to correct Y2K problems. Many times the "fix" will be to replace the device rather than to repair an embedded chip.

3. Mission Critical Systems

For Y2k issues the term "system" includes IT software, hardware, and devices to include microchips.

Mission Critical Systems include those systems:

(a) Defined by the Clinger/Cohen Act as National Security Systems (NSS) (Intelligence Activities; Cryptologic Activities related to National Security; Command and Control of military forces, integral to a weapon or weapon system; systems critical to direct fulfillment of military or intelligence missions).

(b) In direct support of those systems identified by the CINCs which if not functional, would preclude the CINC from conducting missions across the full spectrum of operations including:

(1) Nuclear
(2) Readiness (to include personnel management critical to readiness)
(3) Transportation
(4) Sustainment
(5) Modernization
(6) Surveillance/Reconnaissance
(7) Financial
(8) Security
(9) Safety
(10) Health

(11) Information Warfare
(12) Information Security

(c) Required to perform Department – level and component – level core functions.

4. Army Y2K Management Strategy

a. The Army approach to address the Y2K problem is one of centralized management with decentralized execution focusing our efforts on critical systems. While our primary focus is on critical systems, all Army systems are being addressed including devices and infrastructure. The Director of Information Systems for Command, Control, Communications and Computers (DISC4) as the Army Chief Information Officer (CIO) has overall responsibility for the Army Y2K effort. The Y2K Project Office will facilitate the sharing of information and will monitor Army Y2K progress.

b. Throughout this Plan, the term "system owner(s)" will be used to identify that person, office, or organization responsible for the management and/or correction of Y2K issues for systems and devices. The term "system owner(s)" includes PMs, system managers, item managers, device managers, etc.

c. Some systems require special accreditation or certification, such as those dealing with secure communications and command and control activities. These systems and devices will be recertified, as appropriate, after Y2K corrections have been made.

d. The primary sharing medium is the Army Y2K homepage on the WWW. This sharing of information will include sharing with other DoD and Government agencies as well as the private sector.

e. Additionally, an Army Y2K listserver has been established: Y2KARMY. This is a closed list. Only those who are subscribed are authorized to view archived messages, or to post or receive notes. To subscribe send a request to "army-y2k@hqda.army.mil".

f. The Army tracks Y2K management activities against the criteria and timelines in the Army and DoD Y2K Resolution Process (See Appendix B). The Army will: buy only Y2K compliant products; include Y2K compliance language in all contracts; prioritize system fixes; ensure financial resources are available to address Y2K issues; dedicate sufficient personnel to manage the Y2K effort; assess system risk; plan for contingencies; test systems and devices including interfaces; and certify Y2K compliance. Whenever possible, system owners will consider accelerating fielding dates of new migration systems.

g. Ultimate leadership and resource responsibility remain at the DA FP level because DA FP's are in the best position to determine the critical nature of the software and systems used to accomplish their mission. The majority of reporting responsibility remains with the PEOs, or equivalent level organizations, responsible for each system (see section 15).

h. Date Format:

1) The Army will use the DoD standard date format "YYYYMMDD" ("YYYY" = "four-digit year," "MM" = "two-digit month," and "DD" = "two-digit day") as much as practicable. If a system is Y2K-compliant and does not use the four-digit date format, use of the four-digit year is not required at this time. When interfacing systems are not using the four-digit year format but have procedures in place that allow interfacing systems to operate properly, an exception to the 4 digit year format may be made. These, and all non-standard interface date formats should be used on an exception basis. Regardless of the format, written interface agreements will document date data exchange formats between the interfacing organizations. (See section 14 for more information concerning interface agreements.)

2) If software (a "translator" or "bridge") is to be developed for interfacing systems or databases using different date formats, the system or database using the nonstandard format will pay for the development of the translator or bridge unless otherwise agreed to between the interfacing organizations.

3) In Electronic Commerce, Electronic Data Interchange (EC/EDI) transactions, where other formats are used, the Army will use four-digit year representations when they are available, will use the century indicator ("CC") when it is available, and the Army will use translators/filters as necessary. The century indicator is the first two digits of a four-digit year ("CCYY").

4) Those systems using an ordinal date format must use the format YYYYDD.

i. MAISRC/ASARC Systems: The Army Acquisition Executive (AAE) has directed that systems under the MAISRC/ASARC process address Y2K in all Integrated Process Team (IPT/OIPT). Additionally, their MAISRC/ASARC documents must incorporate Y2K issues as a central theme in the review and acceptance procedures. The Commander of the U.S. Army Operational Test and Evaluation Command (OPTEC) has amplified this guidance and provided additional instructions on evaluation support to new and legacy systems. The OPTEC policy is stated in a memorandum dated 18 July 1997; Subject: Year 2000 (Y2K) Date Processing Problem. A copy of this memorandum is available on the Army "Restricted Homepage".

j. The Chief of Staff of the Army (CSA) has emphasized the importance of reviewing Y2K

impacted systems in an effort to combine or retire unnecessary, duplicative, and legacy systems early. System termination is the preferable solution to repairing a Y2K problem if a risk assessment determines that is a viable option. In some cases, the "window of vulnerability" (period during which dates will be improperly processed) of a system is small, and it may be decided that the system will not be used during that period or that a temporary "workaround" solution can be applied during the "window" and removed afterward.

k. Given the Office of the Secretary of Defense (OSD) guidance of no additional funding for Y2K efforts, reprogramming and use of existing budgets is necessary. The 31 March 1997 Secretary of the Army/Chief of Staff of the Army Top Priority memo states that no system enhancements will be made until Y2K issues are addressed. Y2K efforts may cause delays of some change request proposals or preplanned product improvements. System owners must identify resource shortfalls to the next higher headquarters as soon as possible. They will reprioritize funds to fix critical systems with Y2K problems. (See Appendices L and M for cost information)

5. Installation and Garrison Commanders (CONUS & OCONUS)

a. Installation and Garrison Commanders are responsible for ensuring devices and infrastructures continue to provide service and operate properly on locations under their control. For device or infrastructure element failures, which cannot be avoided, failure mode shall be clearly documented and this information broadly disseminated in order to permit contingency planning to avoid interruption of services. Three categories of devices controlled by information technology are: PCs and servers; communications hardware/software (routers, bridges, switches, PBXs, FAX machines, etc.); and facilities and other systems (biomedical equipment, Heating, Ventilation, and Air Conditioning (HVAC), sprinklers, elevators, security, etc.). Areas of responsibility may include locations off post, leased facilities, and facilities housing tenant organizations. Installation and Garrison Commanders will work closely with local public utility providers on matters concerning continuity of supply of infrastructure services such as electricity, water, communications, etc., and will contact manufacturers of devices such as fire suppression and security systems, heating and air conditioning. (Appendix G provides a guide for checking installation infrastructure)

b. Installation and Garrison Commanders are responsible for ensuring devices affected by Y2K issues are repaired in accordance with the overall timelines in the DoD Y2K Resolution Process (See Appendix B). They will ensure their organizations buy only Y2K compliant products, review all contracts to ensure that Y2K compliance language is included in contracts; prioritize device fixes and replacements, ensure financial resources are available to address Y2K issues, dedicate sufficient personnel to manage the Y2K effort, assess device risk, plan for contingencies, test devices including their interfaces, and certify Y2K compliance.

c. Installation and Garrison Commanders will make awareness of the Y2K problem and its possible personal impact upon the soldier an education, training , and morale issue. The individual soldier must be psychologically and physically prepared for the possible interruption of social and civil services which Y2K may occasion, in order that the soldier may prepare any dependents for such contingencies.

d. Installation and Garrison Commanders are responsible for reporting device information through their MACOM to the Y2K Project Office, IAW the quarterly USAY2KDB reporting requirements. The Y2K Project Office will report the information to DoD.

6. Prioritizing Systems and Devices

a. DA FPs, in coordination with system owners, PEOs and MACOMs, are responsible for prioritizing how systems will be fixed and ensuring mission critical systems receive top priority. Prioritization includes a review of each system to ensure necessary management oversight and resources (funding, manpower, testing facilities, etc.) are available and scheduled in a timely manner. Systems that are critical to the accomplishment of Army warfighting and peacekeeping missions (e.g., weapons systems, and command and control systems) and those that affect the safety of individuals will be given high priority. Additionally, migration systems will receive high priority.

b. Prioritization will be accomplished with close coordination between the DA FPs and the PEOs and system owners, however final decisions rest with DA FPs.

c. Likewise, when prioritizing the correction and testing of devices and infrastructure, priority will be given to those items supporting mission critical systems, or items that affect safety and security.

7. Y2K Risk Management

a. Effective management of the Y2K effort is critical to the Army's ability to continue to perform after 2000. At the heart of the Y2K management program is system and device risk management.

b. Y2K risk management is the practice of applying discipline to the Y2K correction process that will allow you to identify and address risks before they negatively impact a system or device's ability to reach or demonstrate Y2K compliance. Y2K risk management activities include, at a minimum, the identification and assessment of risks, and the planning of contingent or alternative solutions and activities. System and device risk management will consider and protect the interest of the end users as well as the interest of interfacing systems.

c. Risk identification and assessment includes determining how a system or device may fail and what the impact will be: will it stop working; work but not show dates correctly; appear to work correctly but pass incorrect data to interfacing systems. You must determine how a system or device failure will impact the Army's mission as well as your organization's mission, the mission of system users, and the mission of interface systems. The level of risk need to be determined and classified in accordance with guidance in Appendix J.

d. Y2K risk identification and assessment involves a determination of how confident you are that:

- All Y2K issues have been identified
- Fixes for all issues have been identified
- A feasible schedule for fixing and testing the system or device is in place and is being followed
- Resources in the form of personnel, funding, facilities, etc., are available and dedicated to accomplish the fixes
- System testing is fully planned and scheduled, and will be completed on time
- All interfaces have been identified and MOA's are in place
- Interface testing is fully planned, scheduled, and will be completed on time
- The fix and test schedule has included time for unforeseen problems
- A test site is available
- The system or device will be fully operational during Phase V, Implementation

e. Throughout the risk management process, risk identification, assessment, and contingency planning will take place from two points of view—the business area perspective (DA FP responsibility) and system perspective (system manager). Similarly, contingency plans will focus on user impact, and will address contingent actions and impacts from the user perspective and the business area. Risk activities at the system owner level will address individual system or systems (or grouped as defined in paragraph 7.1.).

f. Device risk management activities will be conducted by Installation and Garrison Commanders. These activities will address what actions will be taken if a location does not have heating, security, fire suppression systems, badge readers, traffic lights, or water, for example. Risk management and contingencies can address groups of similar devices, ensuring special attention is given to devices supporting or providing mission critical functions.

g. Contingency planning is the process of identifying proposed courses of action if the Y2K and associated risk control efforts do not achieve the desired outcomes. Contingencies must be planned for the renovation and testing phases as well as the implementation phase. An essential element of contingency plans is the trigger, or execution date that will allow enough time to put the contingency in place, and still meet the Y2K schedule.

h. Contingency plans are prepared based on risk assessments. System and device contingency plans will detail actions that will take place if a proposed Y2K correction fails, is not on time, or if a new migration system is not fielded on time. Contingency plans will consider and address the following:

- How you will accomplish your mission if a system fix or a new migration system is not fielded on schedule?
- Could you do without any part of the system?
- Could any part of the system/subsystem/infrastructure component operations be accomplished manually or under manual control?
- Could the system or device operate with a capability reduction?
- Could the system or function be outsourced?
- Could you turn off the system or device?
- Could a COTS or GOTS product replace the system or device?
- Could you combine the function of a system into another system?
- If you were planning to replace an old legacy system with a new migration system and the migration system is not on schedule, will you be able to fix the old legacy system?
- Have you identified the problems with the old legacy system?
- How long would it take to fix the old legacy system?
- Are resources required to fix the old legacy system available?
- Do workaround plans exist?
- What is the trigger date for putting the contingency plan in action - Again in order to assess the trigger date, a comprehensive schedule must be prepared for system fixes and testing?

i. During the renovation and validation phases, you must also anticipate problems and plan contingencies. The Y2K schedule will not slip—you must consider secondary alternatives in the event your preferred renovation or validation plans cannot be completed. What will you do if:

- The supplier is overwhelmed by the onset of the Y2K crunch and cannot deliver on time and a backup supplier is not available.
- The correction time was underestimated or more resources are required.
- The correction is completed but the system or device just does not work, or you discover a new problem that was not planned for.

j. As outlined above, risk and contingency planning for migration and legacy systems pose a great risk related to the Y2K. The risk centers around the decision not to fix a legacy system because you believe it will be replaced by a compliant migration system prior to 2000. System owners and users must consider and plan as if migration systems will not be available.

k. If your system code or device is simply being modified to correct Y2K issues, risk and contingency planning is still required. Again, as with migration and legacy systems above, you

must consider what will happen if your renovation effort is not completed, tested, or certified on schedule. Your contingencies must address worst-case scenarios.

l. A risk assessment and contingency plan is required for each and every non-compliant USAY2KDB system. It is strongly encouraged that a risk assessment and contingency plan be done for those systems that we think are complaint but have not yet been certified. Risk and contingencies may be addressed in individual plans or by grouping similar systems and devices into a higher level. For example, AMC could write one risk and contingency plan addressing all non critical Business Systems. Risk management and contingency plans may be addressed in one document or can stand as two separate documents.

m. Assessing risk and preparing contingency plans will help focus limited resources and management efforts on those systems that are so critical to the Army mission they simply cannot fail. Based on your results, you may have to reassess the system and device fix priority.

n. A sample risk management worksheet and contingency plan is provided in Appendix J and K respectively. Also see the contingency plan outline at http://www.mitre.org/research/ y2k/docs/ contingency_guidelines.html.

8. U. S. Army Year 2000 Data Base (USAY2KDB)

a. The Y2K Project Office created and maintains the USAY2KDB, which has Y2K information for Army systems. Information in the database is updated and used to prepare quarterly reports that represent the status of Army systems, identify potential problems, and track our progress as we move through the five phase Y2K management process. Initial population of the database began on 30 September 1996 and has continued on a quarterly basis. A USAY2KDB User's Manual, posted to the Y2K Restricted Homepage, provides guidelines for the use of the database.

b. It is critical that every applicable data element be addressed. Every USAY2KDB data element is either required by DoD, OMB, Congress, and the DIST, or is needed to respond to report requirements. Quarterly updates to the USAY2KDB for 1998 are to be provided on 7 January, 7 April, 7 July, and 7 October.

c. The USAY2KDB information is extremely important for tracking progress in solving Y2K problems; identifying compliant systems; sharing system information; ensuring all systems are assessed for Y2K problems; answering Senior Army Leadership, OSD, and Congressional queries; and complying with the DoD requirement to populate the Defense Integration Support Tools (DIST) database. The Army's USAY2KDB automatically feeds the DIST.

d. USAY2KDB data is used to prepare many reports including those that identify:

- Y2K cost (required, expended, allocated)
- Scheduled completion date for each phase
- Number of systems in each of the five phases
- Legacy and migration systems
- Retirement systems
- System status by functional area, i.e. logistics, personnel, etc.
- Device information
- Mission critical systems
- Weapon systems
- Systems using contractor support

e. The USAY2KDB data elements have remained relatively stable since March 1997 when the "one-liner" data elements were added. "One-liner" data includes aggregate information for IT controlled devices and systems that do not meet the criteria to be included as a separate DIST entry in the USAY2KDB. The Y2K Project Office strives to limit the burden of providing additional data, however, once system and device information is entered or baselined, many of the data elements will not be changed at all. Other data elements, such as "Compliance Phase", will change only when there is a change to the information or in the systems status. Common sense must be used to determine which data elements apply to a particular system.

f. All systems, which meet or exceed the following criteria, must be reported as a separate entry in the USAY2KDB. The Y2K Project Office will then report Army Y2K information to the DIST:

- A mission critical system; or,
- A migration system; or,
- A legacy system; or,
- A system with a $2M total cost per year
- A system that interfaces directly with a system that meets any one of the above criteria.

g. Mission critical systems that fall behind schedule must report additional information outlined in Appendix E.

h. All non-mission critical systems reported to the USAY2KDB and DIST are considered to be "major" systems.

9.

One-Liner Systems and Devices Reporting Requirements

a. In addition to the systems described in the previous paragraph, all PEO, separate PM, DA FP's, and/or MACOM systems, or systems belonging to separate activities, not meeting the criteria in paragraph 8, will be entered to the USAY2KDB as a "one-liner" with the following data:

- Number of compliant systems;
- Number of systems non-compliant;
- Number of systems being retired;
- Number of non-compliant systems in each of the five phases;
- Total estimated cost to fix.

b. Furthermore, devices controlled by information technology must also be entered to the USAY2KDB as "one-liner" entries. Three categories of devices controlled by information technology are: PCs and servers; communications hardware/software (routers, bridges, switches, PBXs, etc.); and, facilities and other systems (biomedical equipment, Heating, Ventilation, and Air Conditioning (HVAC), sprinklers, FAX machines, elevators, security, etc.). Aggregate data to be reported are:

- Number compliant;
- Number non-compliant;
- Estimated cost to fix (due to Y2K compliancy, not planned modernization.)

c. In reporting one-liner information to the USAY2KDB cost to replace devices, that are scheduled to be replaced in normal office upgrades and modernization projects, should not be reported. PC cost should include cost of COTS and GOTS office automation software (e-mail systems, Word, PowerPoint, etc.) only if the office automation software was not scheduled to be replaced in normal office upgrade or modernization projects. An exception is when COTS or GOTS is used in the operation, maintenance or support of a particular system or device.

d. Items such as laboratory equipment, mines, night vision equipment, telescopes, calibration equipment, etc., will be reported under the "facilities and other" input unless they are being managed by a PM.

10. USAY2KDB Entry Examples

The majority of the USAY2KDB changes are a direct result of changes in the DIST. Due to the numerous database changes, samples and examples of how different systems should be entered into the USAY2KDB are posted on the Y2K Restricted Homepage and updated as needed, rather than included in this Plan. (NOTE: The examples do not provide entry examples for all pertinent data elements—they addresses a few blocks that have caused confusion in the

past.) You are still required to execute proper reviews and provide information for all applicable data elements that pertain to each system. If sections or modules of a system fall into more than one resolution phase, the system will remain, and be reported as being in a phase until the entire system has completed all activities required by that phase. By now, the database should be totally populated.

11. Compliance Certification Checklist

a. The Certification Checklist guidance has been revised. The completion of the Checklist is now mandatory only for systems reported to the USAY2KDB - including those designated to be mission critical and the remaining major systems. It is highly recommended that the Certification Checklist also be used to document Y2K testing and certification of the remaining one-liner systems and devices, however, this decision is left to the one-liner system and device owners. (See Appendix F)

b. The purpose of the Checklist is to aid system and device owners in ensuring their systems and devices are thoroughly tested, properly documented, and determined to be Y2K compliant.

c. Y2K compliance and validation testing, and completion of the checklist may be done by Contractor or Government personnel. However, Y2K "certification" of Army systems or devices can only be granted by Government employees. Government certification authority for mission critical systems in the USAY2KDB shall be at the General Officer (GO) or Senior Executive Service (SES) level.

d. When positive test results have been achieved and documented for mission critical systems, a copy of the Checklist should be mailed to the Headquarters Department of the Army Y2K Project office.

e. Any USAY2KDB system reported as being in the "Implementation" phase should have a completed Compliance Certification Checklist. A system is not considered to be Y2K compliant until all interfaces properly receive date related data and a completed Compliance Certification Checklist has been signed by the appropriate signatories.

12. Contractual Issues

a. The Defense Acquisition Review (DAR) council released the final definition of Y2K Compliance on 1 January 1997 (see Appendix C). Please note, the definition does not currently cover devices.

b. Per the 8 May 1996 ASD (C3I) memo, the Army will purchase only Y2K compliant products and will issue stop work orders on all contracts for new products being purchased on existing

contracts for products that fail to meet Y2K requirements.

c. The Army will use tailored standard Y2K contract language in compliance with the new and revised direction provided in the 21 October 1997 SARDA Memorandum, Subject Assuring Year 2000 Compliance in Information Technology (IT) Contracts (see Appendix D).

d. Contracting offices will request contractors to develop a Y2K compliance plan to upgrade their Y2K non-compliant products prior to Y2K impacts.

13. Schedule - The Y2K Five-Phase Resolution Process

a. Appendix B outlines the Army resolution process timeline for tackling the Y2K problem. The timelines include milestones for exit criteria from each of the five phases and represent Army "completion targets". Some phases must overlap in order to complete all actions by the end of CY 1998.

b. The Army target for completion of Y2K correction efforts is 31 December 1998. At the system level, target completion is set for 12 months prior to the date the system is expected to experience Y2K-related problems.

c. This aggressive schedule is necessary due to the limiting factor in the Y2K project – Time. This is a high level Army timeline. Subordinate organizations will target these dates for completion of exit criteria and beginning and completing phases, however, it may be necessary to develop your own timeline and exit criteria consistent with the Army's.

14. Interface Agreements

Written system interface agreements in the form of Memorandum of Agreements (MOA's) or equivalent, will be prepared, or existing agreements will be modified to address and document plans for Y2K date transactions. MOA's will include a timeline reflecting when Y2K-compliant data transactions are projected to begin to assist in the preparation of integrating interface testing schedules. The agreements should be prepared to reflect planned information and updated as plans become reality. At a minimum, interface agreements should include or identify:

- Whether interface is input or output
- Current date transaction format
- Planned and actual Y2K-compliant data transaction format
- Planned and actual bridges or filters to be used
- How Y2K compliant date transactions will be tested — when

- How future changes will be made
- Date when Y2K-compliant data can be expected

15. Responsibilities

a. Office of the Director of Information Systems for Command, Control, Communications, and Computers (DISC4) Y2K Project office responsibilities:

1) Oversee Army-wide Y2K management activities and monitor progress.

2) Designate necessary personnel and resources to develop and execute a Y2K oversight program for the Army.

3) Report compliance status to DoD and Army management by organization, highlighting current and potential risk areas.

4) Establish Army-wide strategies and guidance for addressing the Y2K problem.

5) Represent the Army in Y2K matters with DoD and other government agencies.

6) Host In-Process Reviews (IPRs) to review system status and share Y2K information.

7) Establish and maintain the Army Y2K Homepage to act as a clearinghouse for Y2K information and the USAY2KDB information.

8) Own and moderate a closed Army Y2K listserver.

9) Own and operate the USAY2KDB.

10) Based on USAY2KDB data, prepare reports of Army status for OSD and other organizations.

11) Respond to GAO, DoD IG, Congressional, and other inquiries.

12) Represent the Army at DoD Functional Interface Workshops.

13) Establish and update the Army Y2K Action Plan.

b. DA FP (Army Secretariat and Army Staff) responsibilities:

1) Designate necessary personnel and resources to develop and execute a Y2K oversight

program for your functional area. The oversight program will address systems and devices under your purview as well as "FP owned" systems and devices. The Y2K oversight program will include plans to solve Y2K problems, manage system and device risk, and will be consistent with the Army Y2K management strategy and timeline.

2) Facilitate approval of contingency plans when disagreements arise between system users and system owners.

3) In the execution of your oversight program, DA FPs will work closely with system and device owners, PMs, PEOs, and MACOMs, to manage and coordinate your Y2K efforts.

4) Identify a Y2K Point of Contact (POC) to act as the single POC for all Y2K questions and actions within your functional area. The Y2K POCs will pass along Y2K information, memos, direction, documentation, etc. and ensure all subordinate personnel and organizations receive, understand, and comply with Y2K direction.

5) The Y2K POC will stay abreast of the status of Y2K efforts for both systems and devices under your functional purview and will respond to special requests for information from the Y2K Project Office.

6) Prepare a risk assessment and contingency plan addressing your functional business area and the Y2K-impacted systems and devices. Establish trigger dates for implementation of each contingency plan. Coordinate contingency plans with system users. Coordinate on risk assessment and contingency plans prepared by system owners.

7) Ensure the decisions to execute Y2K corrections, replace systems and devices, retire systems and devices, or postpone modifications are consistent with the Army management strategy and the CSA/SA "Top Priority" memo.

8) Make resource decisions and develop funding strategies for systems and devices with Y2K resource problems within your functional area. Identify budget shortfalls and include them in budget submissions.

9) If an issue arises, make final determination of Army Mission Critical systems and prioritization of system and device fixes.

10) Review and monitor quarterly USAY2KDB updates of system and device data within your functional area to ensure data is correct, complete, and submitted on time.

11) Ensure system and device interface agreements, in the form of MOA's or equivalent, have been prepared for systems under your purview.

12) Conduct, direct, track, status, monitor, and/or participate, as required, in Y2K system and device testing. Review and sign the Y2K Certification Compliance Checklist as appropriate.

13) Review all contracts to ensure Y2K language is included and/or modify contracts to add it. Include Y2K language in all new contracts.

14) Purchase and develop only Y2K compliant systems.

15) Ensure exit criteria has been met and is documented prior to moving a system or device to the next resolution phase.

c. MACOM responsibilities:

1) Designate necessary personnel and resources to develop and execute a Y2K oversight program for your MACOM. The oversight program will address systems and devices under your purview. The Y2K oversight program will include plans to solve Y2K problems, manage system and device risk, and will be consistent with the Army Y2K management strategy and timeline.

2) Work closely with DA FPs and MACOM PMs and SMs to manage and coordinate your Y2K efforts, in the execution of your oversight program.

3) Establish a working relationship with interfacing system owners. When possible, coordinate Y2K activities, with the goal being to convert and test related systems simultaneously.

4) Identify a Y2K POC to act as the single POC for all Y2K questions and actions within your MACOM. The POC will pass along Y2K information, memos, direction, documentation, etc., and ensure all subordinate personnel and organizations receive, understand, and comply with Y2K direction.

5) The Y2K POC will stay abreast of the status of Y2K efforts for both systems and devices under MACOM purview, and will respond to special requests for information from the Y2K Project Office.

6) Prepare, or coordinate on the PM-prepared, risk assessment and contingency plan addressing each system and device. The assessment and plan may be at the individual system level, or, several systems may be addressed at a higher level, in an agency overall Y2K plan. Coordinate contingency plans with system users, interfacing system owners, and with DA FP's. The contingency plan must contain a trigger date for its execution.

7) Ensure the decisions to execute Y2K corrections, replace systems and devices, retire systems and devices, or postpone modifications are consistent with the Army management strategy and the CSA/SA "Top Priority" memo.

8) Make resource decisions and develop funding strategies for systems and devices with Y2K problems within your MACOM. Identify budget shortfalls and include them in budget submissions.

9) Identify Army mission critical systems and prioritize system and device fixes.

10) Inventory and report MACOM system and device data in response to quarterly data calls and special requests for information. Report data on time and with complete and accurate information. Ensure data submittals are coordinated with appropriate DA FPs.

11) Ensure MACOM PMs and SMs have obtained, reviewed, and approved documentation that ensures exit criteria has been met prior to moving a system to the next Y2K management phase.

12) Ensure all system and device interfaces are identified and documented in written interface agreements, MOA's, or equivalent.

13) Purchase and develop only Y2K-compliant systems and devices.

14) Review all contracts to ensure Y2K language is included and/or modify contracts to add it. Include Y2K language in all new contracts.

15) Conduct, direct, track status, monitor, and/or participate, as required, in Y2K system and device testing. Review and sign the Y2K Certification Compliance Checklist as appropriate.

16) Ensure exit criteria has been met and is documented prior to moving a system or device to the next resolution phase.

d. Program Executive Officer (PEOs) and Independent PM responsibilities:

1) Designate necessary personnel and resources to develop and execute a Y2K oversight program for systems and devices under your control. The oversight program will address systems and devices under your purview. The Y2K oversight program will include plans to solve Y2K problems, manage system and device risk, and will be consistent with the Army Y2K management strategy and timeline.

2) In the execution of your oversight program, work closely with system DA FP's and PMs to manage and coordinate your Y2K efforts.

3) Establish a working relationship with interfacing system owners. When possible, coordinate Y2K activities, with the goal being to convert and test related systems simultaneously.

4) Identify a Y2K POC to act as the single POC for all Y2K questions and actions within your PEO. The POC will pass along Y2K information, memos, direction, documentation, etc. and ensure all subordinate personnel and organizations receive, understand and comply with Y2K direction.

5) The Y2K POC will establish and maintain a Y2K management program or structure that will enable them to stay abreast of the status of Y2K efforts for both systems and devices under PEO purview, and will respond to special requests for information from the Y2K Project Office.

6) Prepare, or coordinate on the PM prepared, risk assessment and contingency plan addressing each group of devices as a whole. The assessments and contingency plans may be at the individual system level, or several systems may be addressed at a higher level in a logical grouping as described in this Plan. Coordinate contingency plans with system users, interfacing system owners, and with DA FP's. The contingency plan must contain a trigger date for its execution.

7) Ensure the decisions to execute Y2K corrections, replace systems and devices, retire systems and devices, or postpone modifications are consistent with the Army management strategy and the CSA/SA "Top Priority" memo.

8) Make resource decisions and develop funding strategies for systems and devices with Y2K problems within your area. Identify budget shortfalls and include them in budget submissions.

9) Identify Army Mission Critical systems, prioritize system and device fixes.

10) Review, approve, and submit quarterly data updates to the USAY2KDB for systems and devices under your purview. Submit data on time and with complete and accurate information. Ensure data submittals are coordinated with appropriate DA FPs.

11) Ensure PM has obtained, reviewed, and approved documentation that ensures exit criteria has been met prior to moving a system to the next Y2K management phase.

12) Ensure all system interfaces are identified and documented in written interface agreements, Memo of Agreement (MOA), or equivalent.

13) Purchase and develop only Y2K-compliant systems and devices.

14) Review all contracts to ensure Y2K language is included and/or modify contracts to add it. Include Y2K language in all new contracts.

15) Conduct, direct, track status, monitor, and/or participate, as required, in Y2K system and device testing. Review and sign, as appropriate, the Y2K Certification Compliance Checklist.

e. System Owners - Program, Product, Project Managers (PMs):

1) Designate necessary personnel and resources to develop and execute the Y2K resolution activities for systems and devices under your control. Activities will be consistent with the Army Y2K management strategy and timeline.

2) Submit complete and accurate system and device data for the USAY2KDB quarterly update to your PEO, or equivalent office.

3) Obtain, review, and approve documentation that ensures exit criteria has been met prior to moving a system to the next Y2K management phase.

4) Prepare, or coordinate on a risk assessment and contingency plan addressing each system and device. The plans may be at the individual system level, or, several systems may be addressed at a higher level, in an agency overall Y2K plan. Coordinate contingency plans with system users, interfacing system owners, and with DA FP's. The contingency plan must contain a trigger date for its execution.

5) Report potential problems and issues to your PEO, or equivalent office.

6) Ensure all system interfaces are identified and documented in written interface agreements, MOAs, or equivalent.

7) Purchase and develop only Y2K compliant systems and devices.

8) Review all contracts to ensure Y2K language is included and/or modify contracts to add it. Include Y2K language in all new contracts.

9) Conduct, direct, track status, monitor, and/or participate, as required, in Y2K system

and device testing. Review and sign the Y2K Certification Compliance Checklist as appropriate.

10) Ensure documentation is available that reflects exit criteria has been met prior to moving a system to the next Y2K management phase.

f. Installation and Garrison Commanders

1) Designate necessary personnel and resources to develop and execute a Y2K oversight program for devices on your installation or under your control. The Y2K oversight program will include plans to solve Y2K problems and manage device risk and will be consistent with the Army Y2K management strategy and timeline.

2) Ensure the three types of devices (see paragraph 9b) and infrastructure are Y2K-compliant and continue to provide service and properly operate on locations under their control including locations off post, in leased facilities, and in facilities housing tenant organizations.

3) Determine Y2K compliance of all external interfaces with non-IT infrastructure systems, i.e. commercial power, water, communications, etc.

4) Access the ACSIM non-IT web page to check for posted compliance of non-IT systems/equipment (see list in Appendix G) in question before contacting vendors as another installation may already have assessed the same make/model equipment and reported to its MACOM and in-turn to ACSIM for dissemination to all. If not found on the ACSIM web page, contact manufacturers (web page or vendor POC) to determine compliance, cost to make compliant, etc. of devices such as fire suppression and security systems, heating and air conditioning systems, badge readers, etc. Report product findings to MACOM POC for forwarding to OASCIM for inclusion on the non-IT web-site.

5) In the execution of your oversight program, work closely with DA FPs and MACOM PMs and system owners and users to manage and coordinate your Y2K efforts.

6) Identify a Y2K POC to act as the single POC for all Y2K questions and actions within your installation. The POC will pass along Y2K information, memos, direction, documentation, etc. and ensure all subordinate personnel and organizations receive, understand and comply with Y2K direction.

7) The Y2K POC will stay abreast of the status of Y2K efforts for both and will respond to special requests for information from the Y2K Project Office.

8) Prepare risk assessment and contingency plans for all non-IT devices determined to be critical by the Garrison Commander. The assessment and plans may be grouped to address similar devices. Coordinate contingency plans with device users. The contingency plan must contain a trigger date for its execution.

9) Ensure the decisions to execute Y2K corrections, replace, and retire are consistent with the Army management strategy and the CSA/SA "Top Priority" memo.

10) Make resource decisions and develop funding strategies for devices with Y2K problems. Identify budget shortfalls and include them in fund requests to MACOMs for resolution within current resources.

11) Ensure devices supporting mission critical systems or functions and those affecting safety are addressed as a priority.

12) Inventory and report installation device data in response to quarterly data calls and special requests for information. Report data on time and with complete and accurate information.

13) Ensure all device interfaces are identified and documented in written interface agreements, Memo of Agreement (MOA), or equivalent.

14) Purchase and develop only Y2K-compliant devices.

15) Review all contracts to ensure Y2K language is included and/or modify contracts to add it. Include Y2K language in all new contracts.

16) Conduct, direct, track status, monitor, and/or participate, as required, in Y2K device testing. Review and sign Y2K Certification Compliance Checklist as appropriate.

g. ACSIM

In addition to the responsibilities stated in paragraph 15b, act as the single point of contact concerning Y2K non-IT facility infrastructure i.e.(security, traffic lights, HVAC, etc.) issues, establish and maintain information concerning non-IT facility infrastructure product compliance, maintain a non-It status listing at URL (www.hqda.army.mil/acsimweb/ops/y2k.htm) and coordinate Y2K non-IT facility infrastructure product information with MACOMs.

h. DCSINT

In addition to the responsibilities stated in paragraph 15b, act to collect systems and interface

data on classified systems and report it to the ICE-IT database.

i. MEDCOM

Collect medical systems and device information and report same to the Department of Defense (DoD) Health Affairs Directorate for inclusion in the DIST.

j. Army Audit Agency (AAA):

1) Conduct reviews of Y2K management programs and structures at the FP, MACOM, PEO, and PM level to determine if management efforts are adequate.

2) Areas of emphasis and focus are:

- leadership support and awareness
- management and resolution strategies
- individual system assessments
- prioritization of system fixes
- system interfaces
- testing
- risk management and contingency planning

Appendix A: Glossary

calendar errors: errors typically include failing to treat 2000 as a leap year and converting incorrectly between date representations.

compliant: Year 2000 compliant means, with respect to information technology, that the information technology accurately processes date/time data (including, but not limited to, calculating, comparing, and sequencing) from, into, and between the twentieth and twenty-first centuries, and the years 1999 and 2000 and leap year calculations, to the extent that other information technology, used in combination with the information technology being acquired, properly exchanges date/time data with it.

contingency plan: a plan for responding to the loss of system use due to a disaster such as a flood, fire, computer virus, or major software failure. The plan contains procedures for emergency response, backup, and post disaster recovery.

critical system: a system that when its capabilities are degraded, then your organization realizes a resulting loss of a core capability.

Defense Integration Support Tools (DIST): A tool set developed by Defense Information Systems Agency (DISA) to support the DoD-wide information management requirement and provide a migration planning and assessment decision support capability. The D8 Directorate sponsors the DIST. This Directorate is responsible for Modeling, Simulation and Assessments.

extended semantics: in general, specific values for a date field are reserved for special interpretation. The most common example is interpreting "99" in a 2-digit year field as an indefinite end date, i.e., "does not expire." Another is embedding a date value in a *non-date* data element.

data overflow: many software products represent dates internally as a base date/time plus an offset in days, seconds, or microseconds since that base date/time. Hardware integers holding the offset value can overflow past the maximum corresponding date — an event which may lead to undefined behaviors.

inconsistent semantics: at interface between systems, software on each side assumes semantics of data passed. Software must make same century assumptions about 2-digit years.

infrastructure: the computer and communication hardware, software, databases, people, and policies supporting the enterprise's information management function.

integration: two or more software applications that must run on the same physical processor(s) and under the same operating system.

integration testing: testing to determine that the related information system components perform to specification.

interoperability: (1) the ability of two or more systems or components to exchange data and use information. (IEEE STD 610.12); (2) the ability of two or more systems to exchange information and to mutually use the information that has been exchanged.

migration system: a system that absorbs the functions of existing systems, a migration system can be a legacy system or a new system (one that came into existence after September 1991)

outsourcing: paying another company to provide services which an organization might otherwise have performed itself, e.g. software development.

production environment: the system environment where the agency performs its routine information processing activities.

regression testing: selective re-testing to detect faults introduced during modification of a system.

risk assessment: a continuous process performed during all phases of system development to provide an estimate of the damage, loss, or harm that could result from a failure to successfully develop individual system components.

risk management: a management approach designed to reduce risks inherent to system development.

system: an organized assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions. A "system" can be a hardware system, a hardware-software system or a software system. For example, a radar system is an example of a hardware system while a personnel system or payroll system is an example of a software system. This includes but is not limited to ACAT I - IV systems.

systems architecture (SA): a description, often graphical, of the systems solution used to satisfy the war-fighter's Operational Architecture requirement. It defines the physical connection, location, and identification of nodes, radios, terminals, etc. associated with information exchange. It also specifies the system performance parameters. The Systems Architecture is constructed to satisfy Operational Architecture requirements per the standards defined in the Technical Architecture.

Appendix A: Glossary (Cont'd)

system testing: testing to determine that the results generated by the enterprise's information systems and their components are accurate and that the systems perform to specification.

technical architecture (TA): the minimal set of rules governing the arrangement, interaction, and interdependence of the parts or elements that together may be used to form an information system. Its purpose is to ensure that a conformant system satisfies a specified set of requirements. It is the building code for the Systems Architecture being constructed to satisfy Operational Architecture requirements.

test: the process of exercising a product to identify differences between expected and actual behavior.

test facility: a computer system isolated from the production environment and dedicated to the testing and validation of applications and systems components.

unit testing: testing to determine that individual program modules perform to specification.

Appendix B: The Y2K Five Phase Resolution Process

Phase I (Awareness) - Awareness, education, and initial organization and planning take place
-- **Target Completion Date: 31 Dec 1996**
-- Exit Criteria:
---Phase I plan completed and distributed
---Corporate strategies (Army and Functional Proponent levels) developed, submitted to DISC4
---Y2K POCs identified and educated for all organizations within Army, FP, and MACOMs
--- System Users and owners identified and educated
--- Key DOD and industry POCs contacted
--- Phase II plan developed and documented

Phase II (Assessment) - Scope of impact is identified. Device and system level analyses take place.
-- **Target Completion Date: 31 Mar 1997**
-- Exit Criteria:
--- Phase II plan completed
--- 100% of systems & devices, include analyzed for Y2K compliance
--- 100% inventory of all Army systems & devices input into USAY2KDB
--- Phase III plan developed
--- 100% of systems & devices to be replaced, redeveloped, and retired identified and confirmed (Target 01/04/97)
--- Y2K resource plan developed and completed
--- 100% of systems & devices requiring renovation prioritized and scheduled for Phase III
--- Phase IV plan developed
--- Risk management and contingency plan(s) developed

Phase III (Renovation) - Required system & device "fixes" are accomplished
-- **Target Completion Date: 30 Sep 1998**
-- Exit Criteria:
--- Code modifications and revisions completed
--- Appropriate developer testing successfully completed
--- Test planning for Phase IV developed and distributed
--- Phase V Implementation, fielding plan drafted
--- Risk management and contingency plan(s) updated

Phase IV (Validation) - Systems & devices are confirmed. Y2K compliant through assorted testing and certification processes
-- **Target Completion Date: 31 Dec 1998**
-- Exit Criteria:
--- Y2K testing for the system is successfully completed
--- Certification checklist fully and successfully completed
---Y2K system certification signed
---Phase V Implementation, fielding plan finalized

Phase V (Implementation) - Systems are fielded and fully operational after being certified in Phase IV
-- **Target Completion Date: 31 Dec 1998**
-- Exit Criteria:
--- Risk management and contingency plan(s) updated and distributed
--- Systems successfully integrated and operational (Target: 31 Dec 1998)
Note: A subsequent phase may be started prior to the preceding phase being totally completed

Appendix C: Compliance Definition - As of 1 Jan 1997

Introduction: Under the auspices of the Secretary of Defense, the Administrator of General Services (GSA), and the Director of the National Aeronautics and Space Administration; the Federal Acquisition Regulation gives direction and guidance on contract and solicitation procedures for use by contracting officers(KO) and contracting officer representatives (COR) throughout DOD and other federal agencies. The FAR is the authority for the acquisition/procurement of goods and services. The various subordinate levels to the FAR i.e. DoD, HQDA, etc. produce amendments to the FAR known as DFARS and AFARS.

Federal Acquisition Regulations (FAR) - Section 39 - Final 39.002 Definitions.

Year 2000 compliant means, with respect to information technology, that the information technology accurately processes date/time data (including, but not limited to, calculating, comparing, and sequencing) from, into, and between the twentieth and twenty-first centuries, and the years 1999 and 2000 and leap year calculations, to the extent that other information technology, used in combination with the information technology being acquired, properly exchanges date/time data with it.

39.106 Year 2000 compliance.

(a) When acquiring information technology that will be required to perform date/time processing involving dates subsequent to December 31, 1999, agencies shall ensure that solicitations and contracts:

(1) Require the information technology to be Year 2000 compliant; or

(2) Require that non-compliant information technology be upgraded to be Year 2000 compliant prior to the earlier of the earliest date on which the information technology may be required to perform date/time processing involving dates later than December 31, 1999, or (ii) December 31, 1999; and

(b) As appropriate, describe existing information technology that will be used with the information technology to be acquired and identify whether the existing information technology is Year 2000 compliant.

Appendix D: Contract Language

21 Oct 1997

SARD-PP

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Year 2000 Compliance

Because of the concerns expressed throughout Army about whether or not the Government has appropriate and effective remedies in place to ensure satisfactory functionality of information technology equipment between the 20th and 21st centuries, we have developed language which should be incorporated into future solicitations for new information technology contracts. Language is also provided to modify existing information technology supply and maintenance contracts as deemed appropriate.

In addition to the above cited language, the use of warranties is permitted and encouraged if they are used in accordance with FAR Subpart 46.7. This includes tailoring of appropriate clauses such as 52.246-19 and 52.246-20 to indicate that Year 2000 compliance is warranted, and to state that the warranty period runs through a particular date (e.g. December 31, 2002). In addition to the remedies available under the Inspection and Acceptance Clauses (i.e., rejection or pursuit of a latent defect claim), warranty clauses provide other remedies against contractors for nonconforming information technology products or services. Warranties may be cost effective for many mission-critical systems; and the warranty clause may have a defect-prevention effect that is far more valuable than any monetary recoveries that might ever be sought under such clauses.

Use of the solicitation language in conjunction with appropriate use of tailored warranty clauses should provide the flexibility and protection of Government's interests we need in procuring critical information technology products.

Point of contact for this action is Mrs. Esther Morse, DSN 761-1040, Commercial (703) 681-1040.

/S/
John R. Conklin
Director
Procurement and Industrial Base Policy

Enclosure

Appendix D: Contract Language (Cont'd)

Enclosure

SARD-PP MEMO, 21 Oct 1997, SUBJECT: Year 2000 Compliance

RECOMMENDED LANGUAGE FOR INCLUSION IN CONTRACTS FOR COMPUTER HARDWARE, SOFTWARE AND STEMWARE

For new contracts, the contracting office, when soliciting or awarding contracts for newly developed or commercial off-the-shelf products or systems consisting of hardware, software, firmware, middleware, or a combination thereof, shall use the following language, tailored as appropriate, in performance specifications, statements of work, or descriptions of tasks under task order contracts.

The contractor shall ensure products provided under this contract, to include hardware, software, firmware, and middleware, whether acting along or combined as a system, are Year 2000 compliant as defined in FAR Part 39.

For existing IT supply and maintenance contracts, the Contracting Office, when modifying an existing supply or maintenance contract for hardware, software, firmware, middleware or combinations thereof which will continue in use beyond December 31, 1999, shall use the following language, tailored as appropriate, in performance specifications, statements of work, or descriptions of tasks under task order contracts.

The contractor shall accomplish and document modifications necessary to ensure products previously provided, or products to be provided or maintained in the future under this contract, to include hardware, software, firmware, and middleware, whether acting alone or combined as a system, shall be Year 2000 compliant as defined in FAR Part 39.

Appendix E: Y2K Mission Critical System - Late Report

Quarterly OMB and Congressional (Y2K) reporting requirements for all mission critical USAY2KDB systems require reporting of the information below if the system will be replaced or repaired, and has fallen behind the DoD schedule by two months.

a. If this is the first time the system is reported include:

(1) An explanation of why the effort to fix or replace the system has fallen behind and what is being done to accelerate the effort.

(2) The new schedule for replacement or completion of the remaining phases.

(3) A description of the funding and other resources being devoted to completing the replacement or fixing the system.

b. If the system has been previously reported and remains behind schedule include:

(1) An explanation of why the system remains behind schedule and what actions are being taken to mitigate the situation.

(2) A summary of the contingency plan for performing the function supported by the system should the replacement or conversion effort not be completed on time.

A brief (1 or 2 page) status of systems behind schedule, must be reported by the system PEO's, separate PMs, major commands or equivalent offices, or Functional Proponent's, as appropriate, and be transmitted to ODISC4 via e-mail to "army-y2k@hqda.army.mil".

Appendix F: Y2K Certification Checklist

Compliance Checklist Guidance

The purpose of this checklist is to aid system and device owners in ensuring their systems and devices are thoroughly tested, properly documented, and determined to be Y2K compliant. The current definition states "Year 2000 compliant information technology means information technology that accurately processes date/time data (including, but not limited to, calculating, comparing, and sequencing) from, into, and between the twentieth and twenty-first centuries, and the year 1999 and 2000 and leap year calculations, to the extent that other information technology used in combination with such information technology properly exchanges date/time data with it." Additionally, compliant systems or devices have no extended semantics, calendar errors, date overflow, and inconsistent semantics.

The completion of this checklist is mandatory for all systems reported by name (not in the "One Liner Report") to the U.S. Army Y2K Database (USAY2KDB). The Certification Checklist will be used to document the results of Y2K compliance assessments and testing for all USAY2KDB systems - including those designated to be mission critical and the remaining major systems. It is highly recommended that the Certification Checklist also be used to document Y2K testing and certification of the remaining one-liner systems and devices, however, this decision is left to the one-liner system and device owners.

Testing includes unit, integration, system, interface, and acceptance testing. The checklist may be used as a basis for the creation of a Y2K test program. It shall be used for all mission critical developed, COTS, GOTS, gratis, licensed, and purchased software, hardware, middleware, and firmware used in the operation, maintenance, or support of your system or device. The checklist should include references to full test reports or other official documentation related to testing accomplishment, as appropriate.

This checklist applies to all USAY2KDB systems under a development, maintenance, support, test, or any contractual effort. This checklist also applies to systems under Government development, maintenance, etc. The use of this checklist is mandatory for ALL USAY2KDB systems— those with Y2K issues, those determined to be compliant, and those with no date information. For USAY2KDB systems with Y2K issues, provide requested information, attaching additional explanation as required. For USAY2KDB systems with no date information and USAY2KDB systems previously assessed and determined to be compliant, this completed checklist will document that fact. For such systems, ensure the explanation as to how the determination/assessment of compliancy was made is clear.

Compliance Checklist Guidance (continued)

Please note, all interfaces must be tested and data transfer agreements must be documented in writing prior to declaring Y2K compliancy.

Y2K compliance and validation testing and completion of this checklist may be done by Contractor or Government personnel, however Y2K "Certification" of Army systems or devices can only be granted by Government employees. Government certification authority for all USAY2KDB mission critical systems in the USAY2KDB shall be at the General Officer (GO) or Senior Executive Service (SES) level.

This checklist may be used during testing to track the progress of a system or device; however, they are not considered Y2K compliant until positive results have been achieved in accordance with compliance levels outlined in Section 10 of this checklist. When positive results have been achieved, complete this checklist and send a copy to the address below.

This checklist has been updated from the previous version based on user feedback. Either this checklist or the previous version can be used for certification purposes.

DIRECTOR OF INFORMATION SYSTEMS FOR
COMMAND, CONTROL, COMMUNICATIONS, & COMPUTERS
SAIS-IIAC (YEAR 2000 PROJECT OFFICE)
107 ARMY PENTAGON
WASHINGTON DC 20410-0107

Compliance Certification Checklist

1. System or device identification - Provide system/device information, enter N/A where appropriate:

a.	System or device name and DIST #	
b.	Contractor and contract number	
c.	Contractor Program Manager	
d.	Contractor Test Manager	
e.	Testing Organization	
f.	Testing Organization Test Manager	
g.	Date(s) that Year 2000 compliance testing was completed	
h.	Does not process date information - No further action required, see Para 10	
i.	Planned or actual replacement date of tested system or device (retirement or discontinuation qualifies as replacement) if applicable	
j.	For systems or devices with planned replacements, what is the contingency plan if replacements are not available on time, and when, and under what conditions, will it be invoked	
k.	Describe the safety critical portions of the system or device, if any	
l.	Describe recommendations or limitations associated with system or device reintroduction after Year 2000 compliancy is verified	
m.	Describe method of Year 2000 compliance—windowing, patch, bridge, logic change, etc.	
n.	Operational date of system or device (current or future)	
o.	Is all source code available	

Compliance Certification Checklist

2. Internal Date fields - Please provide the following internal date field information:

		YES	NO	N/A
a	System or device use 4 digit year date fields			
b.	If yes to a. is the 4 digit date field in compliance with DoD standard date format — YYYYMMDD			
c.	System or device use 2 digit year date fields			
d.	If 2 digit, system or device uses a century logic technique to correctly infer the century			
e.	If 2 digit, with a windowing technique is it fixed?			
f.	If 2 digit, with a windowing technique is it sliding?			
g.	If yes to e or f , what is the range of dates the date field can represent?			

		Minimum Date	Maximum Date
h.	If windowing is used, describe how proper interfacing with different window values is guaranteed and was confirmed		
i.	At what date will the century logic fix fail?		
j.	Are there any internal data types for dates?		
k.	Input and output internal message formats use 4-digit year data fields in compliance with DoD standard date format YYYYMMDD		
l.	System or device will correctly interpret an internal message received with a 2 digit year.		

Compliance Certification Checklist

3. Year 2000 date processing - Each system or device has its own window of time, before, during, and after the present date, in which it functions. Please indicate if the system or device performed correctly in each of the circumstances described below as a. - g. by checking the "VERIFIED" block. Include reference to a test report or documentation, by page, paragraph number, or whatever is appropriate, that contains the full test information (plans, procedures, results, etc).

		VERIFIED	NO	N/A	TEST RPT REF
a.	Dates in 20th century (1900s)				
b.	Dates in 21st century (2000s)				
c.	Dates across century boundary (mix 1900s and 2000s) – from 1900s into 2000s and from 2000s into 1900s				
d.	Crosses 1999 to 2000 successfully				
e.	Recognized Oct-Dec 99 as FY 2000				
f.	Date forecasting and historical processing between 1900 to 2000 to 1900				
g.	System or device properly process archived data with dates.				

Compliance Certification Checklist

4. Other/Indirect Date Usage - Indicate that you have searched for system or device date information in all of the following examples. Choose NO, if date information was not found; choose VERIFIED if it was, indicating that you found date data and have verified Y2K compliance. Include reference to a test report or documentation, by page, paragraph number, or whatever is appropriate, that contains the full test information (plans, procedures, results, etc).

		VERIFIED	NO	N/A	TEST RPT REF
a.	Dates embedded as parts of other fields				
b.	Dates used as part of a sort key				
c.	Usage of values in date fields for special purposes that are not dates (e.g. using 9999 or 99 to mean "never expire") — extended semantics				
d.	Date dependent activation/deactivation of: passwords, accounts, commercial licenses				
e.	Date representation in the operating system or device's file system (creation dates and modification dates of files and directories)				
f.	Date dependent audit information				
g.	Date dependencies in encryption/decryption algorithms				
h.	Date dependent random number generators				
i.	Date dependencies in firmware				

Compliance Certification Checklist

5. Leap Year - Indicate that you have verified whether the system or device accurately recognizes and processes Year 2000 as a leap year. Include reference to a test report or documentation, by page, paragraph number, or whatever is appropriate, that contains the full test information (plans, procedures, results, etc).

		VERIFIED	NO	N/A	TEST RPT REF
a.	February 29, 2000 is recognized as a valid date				
b.	Julian date 00060 is recognized as February 29, 2000				
c.	Julian date 00366 is recognized as December 31, 2000				
d.	Arithmetic operations recognize Year 2000 has 366 days				

The three rules used to determine leap year are as follows:

Years divisible by four are leap years, unless...

It is also divisible by 100, then it's not a leap year, except for...

Years divisible by 400, which are leap years.

Compliance Certification Checklist

6. Usage of Dates Internally - Internal application usage of dates and date fields must be clear and unambiguous in the context of the systems or devices which use them. Each systems or device has its own window of time, before, during, and after the present date, in which it functions. Please indicate that you have verified the system or device works correctly in each of the circumstances described below described below as (1) - (6) by checking the "VERIFIED" block.

(1)	Dates in 20th century (1900s)
(2)	Dates in 21st century (2000s)
(3)	Dates across century boundary (mix 1900s and 2000s)
(4)	Crosses 1999 to 2000 successfully
(5)	Recognized Oct-Dec 99 as FY 2000
(6)	Date forecasting and historical processing between 1900 to 2000 to 1900

If any circumstance described in para (1) - (6) above is not applicable, so indicate in the N/A block. Include reference to a test report or documentation, by page, paragraph number, or whatever is appropriate, that contains the full test information (plans, procedures, results, etc).

		VERIFIED	NO	N/A	TEST RPT REF
a.	Display of dates is clear and unambiguous (the ability to correctly determine to which century a date belongs either by explicit display, i.e. 4-digit year, or system or user inference)				
b.	Printing of dates is clear and unambiguous				
c.	Input of dates is clear and unambiguous				
d.	Input of logically correct dates				
e.	Storage of dates is clear and unambiguous				

Compliance Certification Checklist

7. External system or device Interfaces - External interfaces must be identified and validated to ensure correct functionality. Each system or device has its own window of time, before, during, and after the present date, in which it functions. Please indicate the system or device worked correctly in each of the circumstances described below as (1) - (6) by checking the "VERIFIED" block. If any circumstance described in para (1) - (6) below is not applicable, so indicate in the N/A block.

(1)	Dates in 20th century (1900s)
(2)	Dates in 21st century (2000s)
(3)	Dates across century boundary (mix 1900s and 2000s)
(4)	Crosses 1999 to 2000 successfully
(5)	Recognized Oct-Dec 99 as FY 2000
(6)	Date forecasting and historical processing between 1900 to 2000 to 1900

The following interfaces must be demonstrated for every circumstance listed in paragraph (1) - (6) above and for every interfacing system or device listed in paragraph a. below. Include reference to a test report or documentation, by page, paragraph number, or whatever is appropriate, that contains the full test information (plans, procedures, results, etc).

		VERIFIED	NO	N/A	TEST RPT REF
a.	Provide a complete and accurate list of interface systems or devices. Include DIST #, system or device name, compliance status, and whether the system or device provides input or receives output.				
b.	Interaction between this system or device and all other external date and time source systems, including GPS, has been verified for correct operation.				
c.	For each interface that exchanges date data, verify that you and the interface organizations have implemented consistent Year 2000 corrections that will correctly work for date data passed between your systems or devices.				
d.	You and each interface organization have negotiated written interface agreements to ensure you have implemented consistent Y2K corrections to enable correct date data passage between your systems or devices.				

Compliance Certification Checklist

8. Year 2000 Testing Information - Please provide the following information with regard to testing the application for Year 2000 compliance. If any responses in this checklist requires additional space, please attach the response to this package, and indicate corresponding paragraph number.

a.	Attach a description of how COTS and GOTS items have been determined to be Y2K compliant			
b.	How was Year 2000 compliance determined (tested in-house, inspected but not tested, etc.)			
		YES	NO	N/A
c.	The test data sets are available for regression testing on the next version release.			
d.	The detailed test results, plans, and reports are available for review and audit.			
e.	A defined process for tracking the status of all Year 2000 problems reported, changes made, testing, compliance, and return to production was followed. Attach a copy or provide an explanation.			
f.	A comprehensive inventory of all systems or devices and system-related components is attached. List includes execution platform, source code, job control, documentation, tools, programming languages, databases, and COTS, Government-Off-the-Shelf (GOTS), and gratis software components as well as the vendor/contractor/organization providing each. If no, provide an explanation.			
g.	Attach an explanation of testing approach for portions of the system or device without source code.			
h.	Attach a description of method(s) used for date simulation (software, unique parameter driver, input fields modified, other)			

Compliance Certification Checklist

9. COTS/GOTS Information - Please provide the following information with regard to components. Include reference to a test report or documentation, by page, paragraph number, or whatever is appropriate, that contains the full test information (plans, procedures, results, etc).

		YES	NO	N/A	TEST RPT REF
a.	System or device use COTS/GOTS application packages and/or infrastructure components				
b.	If yes to a. is a listing of COTS/GOTS items, and their Year 2000 compliance status, attached				
	Narrative Answer				
c.	How was Year 2000 compliance determined? (verified by vendor or contractor, tested in-house, etc.)				

Compliance Certification Checklist

10. Compliance and Certification Levels -

Y2K compliance and validation testing may be done by Contractors. Y2K "Certification" of Army systems or devices can only be granted by Government employees.

Not all systems or devices need to be certified to level 1. The Program, Product, Project Manager and/or the PEO (for PEO managed systems) are responsible for selecting the appropriate compliance level. Compliance levels are defined below. Yes, verified, and N/A, when appropriate, are considered positive responses. No, is considered a negative response.

Government certification authority for all mission critical and ACAT systems in the U.S. Army Y2K Database (USAY2KDB) shall be at the General Officer (GO) or Senior Executive Service (SES) level. The DoD Year 2000 Management Plan directs system developers and maintainers, along with the system's functional proponent, to certify and document each system's Y2K compliance.

LEVEL	DESCRIPTION
0	System does not process date data
1	Full independent testing successfully completed. "Independent" testing is that conducted by an independent Government or Contractor testing organization, such as the Joint Technical Integration Center (JTIC). - All questions have positive responses where applicable
2	Independent audit of system or device and existing test results successfully completed. An "independent" audit is that conducted by a Government or Contractor organization, outside the system or device's chain of responsibility: - All questions have positive responses where applicable
3	Successful self-testing. "Self testing" is accomplished by the system or device, builder, or maintainer (Government or Contractor) in their own facility with no additional review of the system or device or test results. - All questions have positive responses where applicable CAUTION: Self-testing assumes a higher risk level of potential failures
4	System not fielded yet — Y2K compliance contract language is in place

LEVEL OF COMPLIANCE FOR THIS DATA SYSTEM OR DEVICE: (*Circle only one)*

0 1 2 3 4

Compliance Certification Checklist

11. Certification - for Y2K impacted systems or devices -
Signing of this certification indicates the following to be true:
Y2K testing has been successfully conducted for this system or device category. Testing included at a minimum, items listed in this checklist. System or device category has been found to be Y2K compliant. Year 2000 compliant information technology means—"information technology that accurately processes date/time data (including, but not limited to, calculating, comparing, and sequencing) from, into, and between the twentieth and twenty-first centuries, and the year 1999 and 2000 and leap year calculations, to the extent that other information technology used in combination with such information technology properly exchanges date/time data with it." Additionally, compliant systems or devices have no extended semantics, calendar errors, date overflow, and inconsistent semantics.
Y2K compliance and validation testing may be conducted by Contractors, however Y2K "Certification" of Army systems or devices can only granted by Government employees. Government certification authority for all USAY2KDB mission critical systems shall be at the General Officer or Senior Executive Service level. Functional Proponent signature is required for all USAY2KDB systems, except MACOM uniques.

_____ _____
Government System or Device Product/Program/Project Manager (PM) Date
I certify that the information provided in this checklist is true and correct to the best of my knowledge and belief.

_____ _____
Government System or Device Test Manager Date
I certify that the information provided in this checklist is true and correct to the best of my knowledge and belief.

_____ _____
PEO or MACOM Date
Certification Authority (GO/SES level for all ACAT and critical systems)
I certify that the information provided in this checklist is true and correct to the best of my knowledge and belief.

_____ _____
HQDA Functional Proponent (FP) Date
Certification Authority (GO/SES level for all ACAT and critical systems)

I certify that the information provided, in this checklist, is true and correct to the best of my knowledge and belief.

Appendix G: Sample Infrastructure Risk Assessment Guidance

1. Purpose. This document is provided as a sample and guide for developing an installation level Y2K infrastructure non-IT readiness assessment and action plan. This document and the referenced EXCEL Spreadsheet were prepared and are being used by HQ TRADOC. Detailed instructions on completion of the Y2K Non-IT Infrastructure Readiness Assessment Report (EXCEL spreadsheet posted to the Y2K Restricted Homepage) are also included. The spreadsheet is provided as a means to document your non-IT inventory, risk assessment and actions planned, and for summary reporting back to HQDA on a quarterly basis until Y2K.

2. Y2K Problem Background.

a. INTERNET Online References. The Army and TRADOC Y2K home pages provide detailed background information, and links to other top notch federal and commercial Y2K home pages. The TRADOC Y2K home page is linked to a government restricted home page that includes this guidance and associated EXCEL spreadsheet for downloading to your PC, and will list Y2K non-IT POCs, and provide lessons learned as we receive information. We welcome your input to our TRADOC non-IT POC, to share information on vendor's Y2K compliance. You can register on the TRADOC Y2K home page to get automatic notifications when we post new information. INTERNET Universal Resource Locator (URL) addresses:

Army Y2K Home Page:
http:/www.army.mil/army-y2k
TRADOC Y2K Home Page:
http:/www-tradoc.army.mil/dcsim/y2k/index.html

b. TRADOC Y2K Central POCs. Central TRADOC POC for overall Y2K planning, and for IT reporting, is HQ TRADOC, DCSIM, MAJ Dana Barrette, DSN 680-2516, EMAIL:barrettd@monroe.army.mil. Central TRADOC POC for non-IT reporting is HQ TRADOC, DCSBOS, Betty Madison, DSN 680-5032, EMAIL: madisonb@monroe.army.mil. Central TRADOC Engineer POC is HQ TRADOC, DCSBOS, Phil Columbus, DSN 680-2371, EMAIL:columbup@emh10.monroe.army.mil. Central Provost Marshal POC is HQ TRADOC, DCSBOS, Floyd Reneau, DSN 680-4193, EMAIL:reneauf@emh10.monroe.army.mil. Central MWR POC is HQ TRADOC, DCSBOS, Dan Hines, DSN 680-5279, EMAIL: hinesm@emh10.monroe.army.mil. EMAIL communications is encouraged.

c. What Is The Y2K Problem? The Y2K problem is getting worldwide attention as "*The Millennium Bug*" or "*Year 2000 Problem.*"

Appendix G: Sample Infrastructure Risk Assessment Guidance (Cont'd)

This is the first change of century complicated by computers and computer software. Some processor chips and/or associated software utilize a real time clock that only stores the last two digits for the year, and therefore an implied century of 19 is assumed. The majority of microchips manufactured before 1996 do not keep a 4 digit year. On, before, or even after 1 January 2000, any device with microchips (not just PCs, LANs, and software) may malfunction because of the lack of a 4 digit year and/or lack of full Y2K date logic compliance.

d. Army Y2K Plan. The Army established an aggressive schedule for Y2K risk assessment and renovation of all mission essential systems, with a Dec 98 target for validation of full compliance, *within existing resources* (i.e., no central funding). TRADOC installations will certify Y2K compliance to TRADOC, and TRADOC HQ will certify compliance to HQDA (DISC4). Army guidance emphasizes the need to ensure Y2K readiness by *eliminating non-essential systems and equipment by Y2K, and focusing on all critical Y2K issues as a top priority*. The Y2K issue has the attention of the highest echelons of the Army and Nation's top government officials and places responsibility for Y2K infrastructure readiness at the installation management level. Only recently has interest been placed on embedded non-IT systems. MACOMs report Y2K status quarterly to HQDA, DISC4, based on installation input. Installations should report only those costs directly related to ensuring Y2K compliance (e.g., do not report on normal Life Cycle Replacements planned before Y2K). No Y2K funds are set aside by TRADOC or DA.

e. TRADOC's Y2K Information Technology (IT) Readiness Assessment. The TRADOC Change of Century Action Plan initially focuses on traditional information technology (IT): PCs, LANs, custom and COTS software, and communication devices. All TRADOC installations were tasked to develop Y2K risk based action plans by 31 Mar 97. Through the TRADOC Y2K Information Center Web-based forms, installations now have the opportunity to report on local unique automation information systems (AIS) and/or AIS components not reported during prior Y2K data call (e.g., CADD and GIS systems or any other "missed" non-STAMIS/DoD systems). These items are normally purchased through, or provided by, installation DOIMs, who report Y2K status to DCSIM, TRADOC. DCSIM, TRADOC provides quarterly reports to DISC4 on Y2K IT status. DCSIM stresses that they use the Web-based input to capture Y2K impact and support funding decisions.

f. TRADOC's Y2K Non-IT Readiness Assessment. Recent OMB and congressional concern over potentially catastrophic Y2K infrastructure failures resulted in a new MACOM quarterly reporting requirement to HQDA on Y2K readiness of non-IT equipment with embedded chip technology. The TRADOC Change of Century Action Plan

will be updated to

Appendix G: Sample Infrastructure Risk Assessment Guidance (Cont'd)

reflect the Y2K non-IT infrastructure readiness issue.

TRADOC's base operations and mission accomplishment is vulnerable to failures resulting from non-Y2K compliant microchips *embedded* in non-IT devices. Many of these devices are used in facilities management. Non-IT embedded devices are not normally purchased through, provided by, or supported by installation DOIMs. Examples of non-IT devices with embedded chips are traffic lights, Heating Ventilation & Air Conditioning (HVAC) systems, utility control systems, waste/water control systems, and intrusion security control systems. In some cases, equipment or systems are controlled remotely through PCs, which may be relatively easy to isolate, test, and fix/replace. However, microchips embedded inside non-IT devices (e.g., thermostats, smoke detectors, etc) are not obvious, vendor information regarding Y2K compliance is not readily available on the WWW, and microchips cannot always be tested before Y2K by the user for actual Y2K date compliance. These devices may easily be overlooked in a cursory Y2K assessment, but may have *catastrophic operational, safety, and legal impacts* if a device failure occurs. The TRADOC Y2K Non-IT Infrastructure EXCEL spreadsheet is a tool for installations to document their Y2K risk assessment and readiness of non-IT devices, and for initial summary reporting to TRADOC, DCSBOS, by 18 Oct 97, on all mission critical devices. The following update will not be due until Mar 98, to allow time for 100% inventory and reporting.

3. Non-IT Embedded Device/System Definition. For the purposes of the TRADOC Non-IT Readiness Assessment and data call, the definition of *embedded* devices/systems is any non-IT system/device which includes a microchip or microprocessor as an integral part of the operation of that system/device. Y2K compliance and/or lack of date sensitive logic cannot be assumed. With all embedded systems, written Original Equipment Manufacturer (OEM) or maintenance vendor Y2K certification, and follow-up testing will insure 100% Y2K readiness. In general, embedded systems fall within two categories:

a. Microchips, also referred to as "micro circuitry" or "chips" are often *integrated* as part of a standard non-IT device configuration, to assist in operation and/or management of those non-IT devices. Examples are "intelligent" traffic lights, thermostats, and smoke detectors. In these systems, the microchips and associated firmware or software are not normally sold as separate contract line items, and microchips are not normally visible to the end-user or facility manager. Obviously, not all devices with embedded microchips are date sensitive. In many cases, small "intelligent" devices with microchips allow the user to set a 24-hour elapsed time control, or a 7 day calendar which is century independent and will

continue to function properly after Y2K. However, if these devices are not Y2K compliant

Appendix G: Sample Infrastructure Risk Assessment Guidance (Cont'd)

yet rely on full date calculations, *replacement* is often the only option with integrated microchip devices. If these devices are part of a larger component system (e.g., HVAC, fire control systems), the total impact must be assessed.

b. The second category is equipment which is *remotely controlled* or managed by separate PCs/LANs, where the primary purpose of the PC/LAN is to operate or manage those non-IT devices. Examples might include water and sewage flow control systems, intrusion detection systems, and HVAC systems. In these cases, it is fairly obvious to the facility manager that checking the PC for Y2K compliance is required. These systems often keep (date/time stamped) security or maintenance logs, reports, and/or control devices based on a date sensitive logic routine.

c. There are often multiple components requiring Y2K checking and certification in an embedded system, and it can get very complicated to check all components:

(1) Integrated chips inside non-IT device(s)
(2) PC/LAN hardware (Real Time Clock on microchip/motherboard)
(3) PC/LAN software operating system (OS)
(4) PC/LAN COTS software package(s)
(5) PC/LAN custom software package(s)
(6) PC/LAN data files (for system tracking/reporting, etc.)
(7) Y2K readiness of the maintenance vendor servicing the system

Using a HVAC system as an example, it is likely that relatively low "intelligence" (temperature sensor) thermostats will not have a Y2K problem. However, PCs remotely controlling the overall system often require chip(s), and/or operating or remote control software fixes. Sometimes entire systems may require replacement because upgrading individual components and conversion of remote control software and data files (to Y2K 4 digit year) is too costly or labor intensive. In the worst-case, Y2K compliance is *assumed* for a "Y2K problem" system, and on Tuesday, 4 Jan 2000 the workforce will return to a building with an inoperable HVAC system, frozen/broken pipes, damage to office equipment, incur legal repercussions because of damage and injuries from an ungoverned boiler, face multiple safety violations, and the maintenance contractor will be locked out of his own building

because his intrusion detection system failed. Demand certification of full Y2K compliance

Appendix G: Sample Infrastructure Risk Assessment Guidance (Cont'd)

with all new purchases, as vendors themselves may be unaware of Y2K non-compliant chips embedded in non-IT systems (e.g. large HVAC systems). There is a real risk of vendors "unloading" Y2K non-compliant devices to the unaware. Although the installation Directorate of Contracting is the key player to insure contracts with Y2K compliance verbiage, do not underestimate installation managers' role in communicating Y2K requirements with their vendors.

Assume nothing with existing systems, contracts, or contractors. The majority of potential Y2K problems can be avoided by now putting compliance statements in maintenance contracts (e.g., HVAC, elevators, etc), and by requesting written certification of all devices with microchips from OEMs.

4. Non-IT Embedded System/Device Reporting Categories.

a. Excluded Non-IT Embedded Devices. *All installation facilities must be inventoried* for *installation managed devices* (e.g., HVAC, etc.). However, installations need *not* inventory and report on non-IT devices *provided by, and managed by* other MACOMs or organizations. However, meet with the other tenants and responsible agencies to discuss all Y2K issues, and insure *their* scheduling of Y2K fixes does not impact your installation's mission accomplishment, or quality of life of soldiers and civilians. Devices which are *excluded* from reporting on the Y2K Infrastructure Non-IT Readiness Assessment report include:

(1) Installation owned non-IT devices which will be OBE by *Y2K and present no risk of failure from non-Y2K compliance, before system replacement or retirement date.* Do not report devices in buildings/facilities which will be closed by Y2K. Do not report devices supporting other devices in buildings/facilities which will be turned off by Y2K.

(2) Weapons systems centrally managed by AMC.

(3) Aircraft and Air Traffic Control systems centrally managed by AMC and CECOM.

(4) Training and simulation devices centrally managed by STRICOM.

(5) Range control and target control devices centrally managed by ATSC.

(6) Biomedical devices and other hospital equipment centrally managed by

Appendix G: Sample Infrastructure Risk Assessment Guidance (Cont'd)

MEDCOM.

(7) Commissaries centrally managed by DeCA.

(8) Other soldier support organizations (e.g., PXs, Clothing Sales, Class 6 store, gas stations, etc.) centrally managed by AAFES.

(9) Intelligent surveillance devices centrally managed by CID.

(10) Non-IT devices which are an integral part of a centrally managed IT system, such as any time/accounting devices fielded with the Morale Welfare and Recreation.

Management Information System (MWRMIS) by Community and Family Support Center (CFSC).

(11) Traditional office automation and systems owned by the installation, even if used solely for base-level operations and facility management (e.g., CADD and GIS systems, PC/LANs in DPW and DOL, etc.). Report all traditional IT devices (PCs, LANs, communications, COTS and custom software) through your DOIM (see para 2e).

Included Non-IT Embedded Devices. With the exception of devices excluded in the above paragraph, include assessment of all non-IT devices in all *buildings/facilities* on installation real property records, and non-IT devices located on *installation property/grounds*, regardless of whether funded by OMA, OPA, NAF, Army Family Housing, or with tenant funds. The TRADOC Y2K Non-IT Readiness Assessment EXCEL spreadsheet is a partial list of the categories of embedded devices which may be used at installation level. The spreadsheet *is only a starting point.* Your installation probably has other embedded devices/systems not listed. Additionally, it is critical that your installations' training, conus replacement center, and mobilization station (Power Projection/Support Platform) missions are considered as you assess your overall Y2K readiness. Generally, non-IT devices are normally purchased by, developed by, and/or maintained by the installation. Additionally, report on devices maintained by the installation as part of (often reimbursable) services to a tenant. For example, report on DPW maintained HVAC and elevators in a hospital, and on integration of a retail bank's, credit union's, or Commissary's alarm system into an installation-wide security detection system. There are overlapping and "gray" areas of Y2K responsibilities. Although reporting on non-installation serviced devices with microchips in a retail facility on installation property (e.g., fast food restaurants, banks, etc.) is not required, all tenants should be advised to make Y2K an internal management issue now, as it may impact your customer population and a large number

of suppliers and service providers may

Appendix G: Sample Infrastructure Risk Assessment Guidance (Cont'd)

not yet be Y2K aware. If there is a question on whether to report or not, contact the TRADOC non-IT Y2K POC.

5. Installation Y2K Non-IT Readiness Assessment and Action Plan. The army goal is for all installations to be Y2K certified by December 1998. Our goal is to be Y2K "*ready*" with no detriment to mission, soldiers and their families, and civilians. *Simply stated, "ready" means that all devices which have a Y2K problem will be replaced or turned off before a Y2K problem/failure occurs.*

Each installation must develop their total Y2K Readiness Assessment and Action Plan based on their mission, unique environment, and installation management priorities. We know it is a massive level of effort for a 100% inventory of all unique non-IT devices/systems in all installation buildings and facilities. TRADOC will not track devices by facility/building number, however, each installation must keep auditable records on each specific location. TRADOC supports a mission based risk assessment methodology, with the priority for planning, and the 1st report (of a quarterly reiterative reporting process until Y2K) focused on non-IT devices/systems which each installation determines are critical to mission and for the continued safety and high quality of life of installation soldiers, civilians, and tenant customers. The TRADOC Y2K Non-IT Infrastructure Readiness Assessment Report (EXCEL spreadsheet) is a means to document your non-IT inventory, risk assessment, corrective actions, costs, and for summary reporting back to TRADOC. Our recommended approach for developing your Y2K plan:

a. Assign a senior project officer for oversight over total Y2K infrastructure plans, and form a *team* of experts from your DPW, PM, DCA, DOIM, and DPTM to name a few key garrison players.

b. Avoid and/or fix Y2K non-IT problems with FY98/99 contracts (e.g., purchase, maintenance, other services). Now is the time to insure that maintenance contracts for facilities devices include a Y2K compliance clause, and to require Y2K certification from your vendors. Have vendors fix/replace devices in FY98 unless devices will be turned off before Y2K, or if there are major advantages (without mission risk) to wait until FY99 to make Y2K fixes. In some situations, maintenance contractors may experience operational or management difficulties because of their own lack of Y2K readiness. Recommended "Y2K standard contract language" is in the FAR, and may also be downloaded from WWW URL address: http://192.111.52.9/dcsim/y2k/y2klinks.html#ARMY

Appendix G: Sample Infrastructure Risk Assessment Guidance (Cont'd)

c. Focus on the mission critical devices now. Assess the mission impact/severity if a non-IT device/system category fails due to Y2K non-compliance. For the initial report to TRADOC, at a minimum, inventory, check, and report on action required for all devices/systems with mission failure impact/severity of catastrophic or critical (Y2K IMPACT = A or B).

d. Use available free and low cost resources. There are many Y2K home pages on the WWW, and many vendors have their own home page and an EMAIL address to use for asking questions.

Use the WWW to conduct research on Y2K compliance. Local municipal, state, and local colleges may be able to provide no cost/low cost Y2K assistance and/or be tackling the same facilities and infrastructure management issues.

e. Check HVAC, traffic lights and intrusion detection systems soonest, as they have a likelihood of Y2K problems. These types of devices were reported in AMC as Y2K problems.

f. Be sure your senior management is aware of Y2K issues, and subordinate management is aware of the priority to fix Y2K problems. Raise awareness and sensitivity to the Y2K issue by whatever means works at your installation: Commanders Call, special town meetings, posting flyers on bulletin boards, EMAIL, etc.

g. Don't make optimistic assumptions, do understand your legal obligations. Organizations may be aware of Y2K issues, but assume that the Y2K problem will not affect them, and make no attempt to determine if that assumption is justified. You may also contract out Y2K planning, however, this does not negate an installations' legal liabilities associated with Y2K failures.

h. Ensure all traditional automation hardware/software is reported to DOIM. AMC reported that some facilities management automated systems were not included in the initial IT reporting phase (e.g., CADD, GIS). Report IT through DOIM channels to DCSIM.

i. On a quarterly basis starting Oct 97, report to TRADOC, DCSBOS on the TRADOC Y2K Non-IT Infrastructure Readiness Assessment Report (EXCEL spreadsheet).

j. Certify by Dec 1998 full Y2K compliance. Army certification checklists may be downloaded from the WWW TRADOC Y2K homepage.

6. TRADOC Y2K Non-IT Infrastructure Readiness Report (EXCEL spreadsheet). This spreadsheet will document your plan by documenting the inventory of non-IT devices, Y2K impact, corrective action, and costs for each type of device. Additional rows may be inserted for specific devices. You will probably not have information for all data fields (spreadsheet columns) initially. Complete what you can for the initial submission, and refine your report in subsequent quarterly submissions to TRADOC, as you take corrective actions to fix Y2K problems. Data field definitions and examples follow:

a. Y2K Fail Prob (Y2K Failure Probability). Assess the probability/ likelihood of a Y2K failure with devices/systems.

For example, Y2K compliance of an elevator may be unknown, however you may assess the probability as code 5 because this elevator is not remotely controlled, has no automated maintenance tracking, is not programmable at the control panel, and initial telecon to maintenance vendor confirms there is probably no Y2K failure issue for that specific make/model.

Code: Definition:
1 - Device/System will fail in Y2K
2 - Unknown, extremely high probability of failure
3 - Unknown, high probability of failure
4 - Unknown, moderate probability of failure
5 - Unknown, low probability of failure
6 - No Y2K failure (device Y2K "compliant" or Y2K "ready", manual work around, or Y2K is a non-issue for that device

b. Y2K Impact. Assess the *mission impact/severity* if the device/system fails due to Y2K non-compliance. Refer to Army FM 100-14, Risk Management, pages 2-8 for detailed definitions of severity codes. For example, a malfunction of a HVAC system may have catastrophic mission, safety and legal impacts in a hospital or child care facility, and marginal impact in a "lights out" warehouse with no climate sensitive equipment. Multiple spreadsheet rows may be used for one device/system, if there is different mission impact. Installation level Y2K priorities and resourcing decisions should be made based on Y2K FAIL PROB and Y2K IMPACT codes. That is, devices with a code combination of 1A, 1B, 2A, 2B, 3A, 3B, 4A, and 4B should receive high installation priority for Y2K fixes.

Code: Definition:
A - Catastrophic
B - Critical
C - Marginal
D - Negligible

E - None

Appendix G: Sample Infrastructure Risk Assessment Guidance (Cont'd)

c. Manufacturer, Make/Model Number, Manufacturer POC Name/Phone Number. Self explanatory. For internal records, also track serial numbers. Some vendors may have different microchips in the devices with the same manufacturer, make, and model number. In the PC industry, it is standard for vendors to track microchip and firmware based on serial numbers. Do not assume that because there is no Y2K problem with one make/model number, that all the manufacturer's other products will be OK.

d. Number of Systems. Enter number of devices/systems for a specific category as defined by fields 6a-c above. Number of actual devices is normally appropriate (e.g., number of traffic lights). For systems which have many component devices with embedded microchips (e.g., HVAC), number of total integrated systems is appropriate.

e. Number of Facilities w/Systems. For the report to TRADOC, enter the number of facilities/buildings involved for a specific category as defined by fields 6a-c above. TRADOC does not plan to track readiness by building number at this time. However, installations must track this information and are encouraged to use a duplicate spreadsheet to maintain building/facility numbers for all devices inventoried.

f. Action (Corrective Action). Enter the corrective action.

Code: Definition:

C - Completed
F - Fix
R - Replace
E - Eliminate
M - Manual workaround
N - No action required
U - Unknown (To Be Determined)

g. Action FY. Enter the FY of corrective action.

h. TRADOC Cost ($K) (to correct). Enter your total cost, in $K, to correct a Y2K problem for the total number of a specific device/system reported. Enter zero if no cost. Leave blank if unknown. Do not include costs for which you are reimbursed by customers (e.g., tenant activities). Do not include normal recurring maintenance and/or life cycle replacement costs.

i. Other Cost ($K) (to correct). Enter the cost, in $K, to correct a Y2K problem for the total number reported of a specific device/system, for which you are reimbursed, or when other non-installation organizations pay directly (not through your installation) to vendors. Enter zero if no cost. Leave blank if unknown.

j. Notes. Indicate all *"showstoppers"*. As appropriate, include pertinent information regarding problem description, funding appropriation information, POC device supports, and/or additional device information.

k. Typical Non-IT Systems. Embedded controllers may be found in the following kinds of systems. This list does not purport to be exhaustive.

Office systems and mobile equipment:
- Telephone systems/answering machines/voice mail
- Fax machines/copying machines
- Time recording systems
- Mobile telephones
- Still and video cameras

Building systems:
- Lighting systems
- Backup lighting and generators
- Fire control systems
- Heating and ventilating systems (HVAC)
- Elevators, escalators, lifts
- Security systems/security cameras
- Closed circuit TV systems
- Access control systems
- Safes/vaults/door locks
- Landscaping systems (sprinkler/irrigation)

Manufacturing and Process Control:
- Manufacturing plants
- Water and sewage treatment systems
- Power stations/power grid systems
- Oil storage facilities
- Simulators
- Test equipment used to program, monitor and test control systems
- Shelf life calculations
- Ordering systems to include acceptance/distribution

Transportation:

- Airplanes/trains/buses/marine craft/automobiles/trucks, etc.
- Air traffic/rail traffic control systems
- Signaling systems
- Radar systems
- Traffic lights
- Ticketing systems/machines
- Car parking meters
- Command and control systems
- Emergency equipment
- Photo surveillance systems

Banking, finance and commercial:
- Automated teller machines (ATM)
- Credit card systems
- Point of sale systems including scanner/cash systems
- Payroll/retirement
- Vending machines

Other monitoring systems:
- Energy metering
- Environmental monitoring equipment
- Training rectification
- Chemical exposure
- Equipment calibration
-Air/water quality

Appendix H: Sample MOA (Interface Agreement)

MEMORANDUM OF AGREEMENT
BETWEEN YOUR SYSTEM AND THE INTERFACING SYSTEM(S)

1. PURPOSE - This MOA documents how (your system) and (the interfacing system name) will manage the Y2K correction process and exchange date information to allow the systems to send and receive and correctly process date information leading up to and after 2000. This MOA includes a timeline reflecting when Y2K compliant data transactions are projected to begin and addresses interface testing. This agreement reflects planned information and is updated as plans become reality. Interface agreements should include or identify:

2. BACKGROUND - Briefly define interface relationships, whether the interfaces are currently compliant.

3. SENDING SYSTEM
   CURRENT FORMAT
   PLANNED FORMAT

4. RECEIVING SYSTEM
   CURRENT FORMAT
   PLANNED FORMAT

5. PLANNED CORRECTIVE ACTIONS - Describe planned corrective actions. Include windowing parameters, bridges, filters, etc. that will be in use, if applicable.

6. SCHEDULE - Outline the proposed renovation schedule

7. PROGRESS REVIEWS - Define how parties of the MOA will be appraised of progress in the accomplishment of the corrective actions.

8. INTERFACE TEST ISSUES - Outline interface testing plans and schedule

9. EFFECTIVE DATE - List the effective date when Y2K compliant data is expected to begin

10. FUTURE ACTIONS & AMENDMENTS - Describe future required actions

SYSTEM NAME	INTERFACING SYSTEM NAME
SIGNATURE/DATE	SIGNATURE/DATE

Appendix I: Sample Y2K Risk Management Plan

The Risk Management Plan presents the overall approach to managing risk during the Y2K renovation effort and controlling the residual risks that may be experienced by the operational users of the renovated system or systems. The plan contains both strategic and tactical aspects to answer six questions associated with identifying, assessing, and handling risk:

1. Why? The purpose and objectives of the risk management program;
2. How? The approach that will be used to identify, assess, and handle risks;
3. Who? The organizational and individual responsibilities for accomplishing the risk management function;
4. When? The schedule elements associated with the plan;
5. What? The technical elements associated with the plan; and
6. How Much? The budget/cost elements associated with the plan.

From the strategic perspective (the Y2K renovation effort for a program or system), the plan addresses the organizations overall commitment to and strategy for risk management. From a tactical perspective (the specific risks associated with the Y2K renovation effort for a program or system), the plan addresses the specific options and selected approach to specific risks. The following presents a sample outline for the strategic and tactical elements of a Y2K Renovation Risk Management Plan.

1. Strategic Components

I. Introduction (This section answers the "why" element and provides an overview of the "how" elements.)

Purpose: Describes the risk management strategy and process. Documents organization and methods.

Objectives: Describes how you will:

- Resolve risk
- Maximize project control

Overview: Provide a document summary

II. Strategy (This section answers the "how" and provides an overview of the "who" elements.)

Policy: Defines if the strategy described applies for all programs; for all Y2K resolution phases.

Organization:	Defines roles and responsibilities.
Approach:	Defines a proactive, quantitative, integrated, and systematic approach

III. Process (This section refines the "how" in additional detail and answers the "what" elements.)

Risk:	Describes the process for identifying and assessing risks
Contingency planning:	Describes the approaches and preferred alternatives for handling risk

IV. Verification (This section describes the method for verifying that the "what" elements were successfully implemented.)

Metrics:	Identifies the metrics and/or indicators that provide quantitative targets with warning levels for implementing risk handling alternatives.
Reports:	List top-10 risks.
Reviews:	Describes management reviews associated with the risk management effort.

V. Resources (This section answers the "who," "when," and "how much" elements.)

Staff:	Identifies the numbers and skill levels required.
Schedule:	Defines the schedule and identifies any slack
Budget:	Identifies the management reserve available.
Availability:	Describes whether required resources are readily available.

2. Tactical Components (sample for a potential risk)

Tactical Risk Management Plan for "Creeping Requirements"

Why?	Our analysis found that the average requirements overrun on our projects is about 40%. We need to control creeping requirements to prevent uncontrolled cost and schedule increases on the renovation effort.
How?	In general, we looked for ways to eliminate the source of requirement changes by baselining the requirements. After that, we verified that only those requirement changes that are absolutely necessary were added to the baseline.
What?	We are addressing the risk in three specific ways: 1. We're using a **user interface prototype** at the beginning of the project to be sure we gather high-quality requirements. We will continue showing the prototype to the users, refining it, and showing the prototype to the users again until we are confident that they will be very happy with the software we build. 2. We're **placing the requirements specification under explicit change control**. After we complete the user interface prototype and gather other

requirements, we'll baseline the requirements. After that, requirements changes will have to go through a more formal change process in which cost, schedule, quality and other impacts have to be carefully assessed before the change is accepted.

3. We're using a **staged delivery approach** to keep the delivery cycles short, which reduces the need for changes within cycles. Between stages we can change features if needed.

We'll upgrade this risk to a higher level if any of the following conditions become true:

- We can't get users to buy into a user interface prototype within a reasonable amount of time.
- We receive requests for requirements changes constituting more than 5% of the system in the first 30 days after the requirements have been baselined.
- We accept requirements changes constituting more than 5% of the system at any point in the renovation life cycle.

Who? The **engineering lead** is responsible for the user interface prototype.
The **change board** is responsible for maintaining the requirements under change control.
The **renovation manager** is responsible for keeping the stages within our staged delivery plan short.

When? We'd like to have the UI prototype complete by 4/15. If it isn't complete by 6/1, we'll upgrade the severity of this risk to "project critical."
The requirements spec should be baselined by 5/15. If it hasn't been baselined by 6/15, we'll upgrade the severity of this risk to "project critical."
We should have completed our first staged delivery by 7/15. If it hasn't been completed by 8/15, we'll upgrade the severity of this risk to "project critical."

How much? We estimate the UI prototype will cost 6 engineering staff months. Explicit change control is accounted for in our standard development practices and does not add cost to the project. Staged delivery increases the apparent project cost by about 5% because of the increased effort associated with releasing the software multiple times, but it reduces integration risk and the risk of building the wrong product. In the end the only increase is probably in the visibility of project's true cost, so it is a net gain rather than a cost.

Introduction

Purpose - Describe risk management strategy and process. Document organization and methods

Objectives - Describe how you will:

Resolve risk

Maximize project control
Overview - Provide a document summary

Strategy

Policy - Does strategy described apply for all programs; for all Y2K resolution phases
Organization - Define roles and responsibilities
Approach - Define a proactive, quantitative, integrated, and systematic approach

Process

Risk - Identify, assess risk
Contingency planning- Identify actions to overcome/offset risk

Verification

Metrics - include quantitative targets with warning levels
Reports - list top-10 risks
Reviews - Describe management reviews

Resources

Schedule - Define schedule and slack
Budget - Management reserve available
Staff - Adequate numbers and skill level
Availability - Are required resources readily available

Appendix J: Sample Y2K Risk Management Worksheet

Information Resource Item:
(Organization, System, Application, Hardware, Firmware, Software, Equipment, etc.)

Year 2000 POC:
(Name, location, phone and e-mail address)

Organization (PEO Staff or PMO) **& Location:**

Business process, function, or mission affected:

Risk:
Sentence or short paragraph defining the risk

Level of Risk: ____Catastrophic _____Critical _____Marginal ____Negligible ___None

Catastrophic--The problem will cause a total failure of one or more missions

Critical--The problem will cause major disruptions in ability to perform its mission

Marginal--The problem will cause errors and impact the mission

Negligible--The problem is minimal, an inconvenience

None--Y2K has no impact on the information resource's functionality

Alternatives:
Describe optional courses of action

Resource Requirements & Implications:
Describe for each alternative; include time and materials and the impact on other projects

Priority:
Priority is the relative import of the information resource to the mission. In developing a measure of priority, consider not just the resource itself, but other Army businesses or functions which may depend on it. For example, an operating system may not appear to be high priority, but the logistics systems which runs on it are critical, therefore, the operating system becomes critical as well.

Actions to Mitigate Risk: Describe alternative which will be implemented.

Relationship to other information resources & other business-functions: Describe relationship to interfacing systems and business functions.

Appendix K: Y2K System or Device Contingency Plan Outline

Contingency Plans (CPs) are needed to ensure critical missions are not adversely impacted by the Year 2000 Century change. Each System or Device should have its own CP, though systems with similar functions may be grouped together when appropriate.

I. Renovation Y2K System or Device Contingency Plan Outline

Renovation contingency planning deals with alternatives to reduce and/or control risk and focuses on actions if renovation efforts won't be completed on time and/or a particular renovation associated change fails in the operational environment. At the MACOM level, consideration should be given to how the Army's mission will be impacted by the loss of one or more mission critical Systems. If a CP is already in place, it may be modified to address the Y2K issue. The following is a sample renovation contingency plan outline.

Section 1. PURPOSE – This plan identifies risks, potential contingent activities, and responsibilities for putting contingent plans into effect in the event that planned Y2K correction activities are not successfully accomplished for the ABC System.

Section 2. BACKGROUND - Briefly describe Y2K correction and risk management activities.

Section 3. SYSTEM OR DEVICE MISSION - Describe system or device mission.

Section 4. RESPONSIBILITIES - Identify responsibilities of all concerned and impacted parties including interfacing system and device owners, systems and device users, and DA FP's.

Section 5. IDENTIFIED RISKS AND CONTINGENCIES FOR EACH PHASE - Include categorized risks for each phase as listed below. Identify contingencies, solutions, and workarounds for each risk identified. Identify trigger or start dates for putting each contingent plan in place. Identify impact of contingencies in place. Address items such as degraded system functionality, additional training to accomplish a manual workaround, additional personnel requirements, etc.

INDICATORS/METRICS - Contains the indicators/metrics that will be used to trigger implementation and verify successful implementation of the contingency plan.

RENOVATION PHASE - You may use the Y2K risk management worksheet in Appendix M to identify risk. In the determination of risk, address the items listed in paragraph 7 of this Plan.

TEST AND VALIDATION PHASE - You may use the attached Y2K risk management worksheet in Appendix J to identify risk. In the determination of risk, address the items listed in the pertinent paragraph of this Plan.

OPERATIONAL PHASE - You may use the attached Y2K risk management worksheet in Appendix M to identify risk. In the determination of risk, address the items listed in paragraph 7 of this plan.

COMMUNICATIONS - Identifies all applicable internal and external communication systems that are necessary to successfully implement the contingency plan.

INTEGRITY AND SECURITY - Defines the specific activities necessary to ensure that required integrity and security levels (access, data manipulation, and communications) are maintained following implementation of the contingency plan.

Section 6. IMPACTS TO INTERFACING SYSTEMS - Identifies impacts to interfacing systems. Identifies the hardware, software, communications, and process interfaces affected by the contingency plan.

Section 7. IMPACTS TO USERS - Identify impacts to system and device users.

Section 8. COORDINATION - Obtain coordination from system users, system DA FP's, and interfacing system managers.

PURPOSE - This plan identifies risks, potential contingent activities, and responsibilities for putting contingent plans into effect in the event that planned Y2K correction activities are not successfully accomplished for the ABC System.

BACKGROUND - Briefly describe Y2K correction and risk management activities

SYSTEM OR DEVICE MISSION - Describe system or device mission

RESPONSIBILITIES - Identify responsibilities of all concerned and impacted parties including interfacing system and device owners, systems and device users, and DA FP's.

IDENTIFIED RISKS AND CONTINGENCIES FOR EACH PHASE -
Include categorized risks for each phase as listed below. Identify contingencies, solutions, and workarounds for each risk identified. Identify trigger or start dates for putting each

contingent plan in place. Identify impact of contingencies in place. Address items such as degraded system functionality, additional training to accomplish a manual workaround, additional personnel requirements, etc.

RENOVATION PHASE - You may use the Y2K risk management worksheet in Appendix M to identify risk. In the determination of risk, address the items listed in paragraph 7 of this Plan.

TEST AND VALIDATION PHASE - You may use the attached Y2K risk management worksheet in Appendix J to identify risk. In the determination of risk, address the items listed in the pertinent paragraph of this Plan.

OPERATIONAL PHASE - You may use the attached Y2K risk management worksheet in Appendix M to identify risk. In the determination of risk, address the items listed in paragraph 7 of this plan.

IMPACTS TO INTERFACING SYSTEMS - Identify impacts to interfacing systems. Be prepared to update interface MOA's, if necessary, to reflect interface changes when contingencies are put into action.

IMPACTS TO USERS - Identify impacts to system and device users.

COORDINATION - Obtain coordination from system users, system DA FP's, and interfacing system managers.

Appendix L: Y2K Cost Estimating Guidance

The purpose of this guidance is to develop a rough order of magnitude of cost to find, fix, and test systems for the Y2K problem. This estimate does not include costs to make the systems' hardware and "system's software" (commercial hardware and software associated with the system) Y2K compliant. These are additional costs which can be significant, especially if there is a requirement to produce a microchip (piece of firmware).

"While an exact estimate cannot be determined until an in depth analysis has been completed, rough metrics (plus or minus 40 percent of actual project costs) can be applied to the application inventory..."

"...Estimates include project management, labor costs, locating and identifying affected code/data, parsing and analyzing for affected code data; determination of options, implementation of solutions, unit and integration, testing, and implementation..."

"...Note that integration testing can be half of the overall cost estimate due to the nature of the solution and the need to develop and/or update current regression test beds to exercise modified date routines..."

- *Gartner Group, Key Issue Analysis, KA-210-1262, B. Hall & K. Schick*

Cost Estimating Technique

The following estimate techniques are based on the formulas developed by the ***Gartner Group***, an independent advisor to business professionals making information technology (IT) decisions. **Applying this technique requires an accurate system inventory which includes source lines of code (SLOC).**

A 2-step process can be used to produce a rough order of magnitude for system applications.

Step 1: Multiply SLOC times .80. This approximates the number of executable lines of code (ELOC). The 0.8 is a "rule of thumb" constant based on experience.

Step 2: Multiply your ELOC times the cost per LOC.

Appendix L: Y2K Cost Estimating Guidance (Cont'd)

Range of Estimated Cost per LOC

The MITRE Corp. recently released the following cost estimates in an effort to help DoD services and agencies develop rough orders of magnitude. These estimates are based on MITRE's analysis of a representative sampling of DoD source code.

Ground and Airborne Radar Systems:	$2.02 - $8.52 per LOC
Communications Processing Systems:	$1.23 - $5.54 per LOC
C2 Planning Systems:	$1.22 - $1.84 per LOC
Logistics Support Systems:	$1.02 - $1.39 per LOC
AIS Systems:	$0.75 - $1.70 per LOC

The Y2K Cost Factors Checklist at Appendix M lists the factors that drive costs per LOC. These factors should be considered in determining what is the appropriate estimated cost per LOC within the range.

Other Estimates

A labor rate of $10K/Staff Month (contract services support) is a reasonable planning estimate for equating dollars to staff months of work effort.

An estimate of staff years per Million LOC is 10 staff year/ 1 Million LOC

Appendix M: Y2K Cost Factors Checklist

There are many factors which affect the estimate of Y2K fixes. These factors are enumerated here to consider in determining total costs. Your estimate should be adjusted based on knowledge of the system(s) and the relevance of these factors.

NOTE: Y2K "compliancy" includes proper processing of Leap Years [The Y2K is a Leap Year.]

Application Software:

___Size: Number of executable lines of code (ELOC)

___Age: Older code tends to be less structured and thus harder to understand

___Complexity: Relative intricacy/understandability of business rules

___Documentation: degree of documentation available and its understandability

___Programmer: Familiarity with the program code. Level of skill/competency/expertise.

___Source Code: Availability

___Date-"Intensiveness": Relative number of date related calculations/comparisons

___Embedded Dates: Frequency of date use as part of data element or in data element codes

___Date Formats Used: Consistency within the system of a standard date format

___Y2K Strategy (field expansion/procedural code/sliding window): Different strategies to achieve Y2K "compliancy" have different costs

___Language: Some languages (e.g., COBOL 68) are unable to properly process the Y2K so the software will have to be upgraded/changed. [Additionally, the language relates to the availability of Y2K COTS tools, programmers to work on the system, and availability of Y2K compliant COTS]

Hardware/System Software:

___Y2K Compliancy of Each of the Components of the Technical Environment is Required. [Often only a current version of a product will be Y2K compliant.]

___Operating System

___Major Subsystems: Sometimes subsystems have different technical environment components

___Database Management System (DBMS)

___Compilers/Cross-Assemblers (available — sometimes they don't exist)

___Teleprocessing (TP) Monitors

___Homegrown/Locally Developed Software: Software used in conjunction with the system

___Workstation Software: Consider the quantity needed

___Workstation BIOS (handles the "system clock function"): 60%-80% of PC BIOSs are not Y2K compliant — most are soldered to the "motherboard," some are reprogrammable, some are "socketed" and can be replaced

___Programmer: Familiarity with the hardware and operating system. Level of skill/competency/expertise.

Appendix M: Y2K Cost Factors Checklist (Cont'd)

__Programmer System Software (utilities and development tools): To support making changes to the software

___Capacity/Usage Level: Making a system Y2K compliant may increase storage (DASD) requirements or even CPU requirements and cause a need to purchase a larger computer or more DASD.

___Embedded Software (microchips/circuit cards; e.g., PBXs, security system (access control), cash registers): They may be directly or indirectly related to a system, and may not be Y2K compliant. The availability of compliant hardware or the cost of developing it, and the quantity required must be considered.

___Communications: Telecommunications hardware and software upon which the system depends must be considered

___Network Timestamps (LAN/WAN network clock time): Upon which the system is dependent

Databases/Files:

___Number of Date-Related Data Elements

___Amount of Available DASD (storage space)

Y2K Tool Support:

___Availability: Many languages and/or technical environments do not have Y2K COTS tools so tools must be developed in-house or specifically contracted for development

___Quality

External Interfaces/Middleware:

___Data Sources: Must be evaluated and "bridges" planned as required

___Data Outputs: Must be evaluated and "bridges" planned as required

___EDI Transaction Sets: System may generate some EDI transactions or get input from EDI transactions which may require "bridges"

___Reports: System may generate paper reports which need to be modified

___Screens: System may have user screens which require modification

Appendix M: Y2K Cost Factors Checklist (Cont'd)

System Plans:

___Planned Major Upgrade: May be used to do Y2K compliance work at the same time to reduce costs

___Termination: System may be eliminated before a Y2K problem occurs

___Replacement: System is planned for COTS replacement or reengineering before a Y2K problem

Miscellaneous System-Related Information:

___Sort Routine Y2K Compliancy

___Backup Routine Y2K Compliancy

__Archival Routine Y2K Compliancy

___System Criticality/Priority: Really not required for cost estimate, but a good time to record this critical planning information

___Risk Analysis If System Fails: Really not required for estimating cost, but a good time to collect this critical planning information. Consequences of system failure must be considered

___Risk Analysis (if system not made Y2K compliant): Many systems only have a small "window of vulnerability" during which the inability to properly process Y2K occurs. Consideration must be considered if this "window" is acceptable; i.e., the system won't be used during that period, or a "workaround" will be established for that period; e.g., manual processing.

___Contingency and Continuity of Operations Planning

Y2K Management:

___Project Management

___Configuration Management

___Change Management

___Contract(or) Management

___Y2K Emergency Reaction Team

___ Risk Management

Y2K Testing:

___Establishing Test Environment

___Unit Testing

___Integrated Testing

___Y2K Simulation Testing: Can sometimes require mirror of production environment. Might not be possible until technical environment is made Y2K compliant

___Risk Management